Q001 1-1 IT基盤 / OS・ハードウェア

オペレーティングシステム（OS）の役割として、最も適切なものはどれか。
ア．利用者が入力したデータを必ず暗号化して保存する。
イ．ネットワーク上の全通信経路を一元的に決定する。
ウ．アプリケーションごとの業務ロジックを自動生成する。
エ．CPU、メモリ、入出力装置などの資源を管理し、アプリケーションに利用環境を提供する。

正答・4肢解説・総合解説

正答：エ．CPU、メモリ、入出力装置などの資源を管理し、アプリケーションに利用環境を提供する。
ア：暗号化はOSが提供できる機能の一つだが、全データを必ず暗号化することがOSの基本役割ではない。
イ：通信経路の決定は主にルータなどのネットワーク機器の役割であり、OSの一般的な基本役割とはいえない。
ウ：業務ロジックはアプリケーション側で実装されるもので、OSの基本機能ではない。
エ：OSはハードウェア資源を抽象化・管理し、プロセスやファイル、入出力などの基本サービスを提供する。
総合解説：OSはハードウェア資源の管理と、アプリケーションがそれらを安全かつ効率的に利用するための共通機能を提供する。セキュリティではプロセス分離や権限管理も重要となる。

Q002 1-1 IT基盤 / OS・ハードウェア

一般的なOSにおけるプロセスとスレッドの関係として、最も適切なものはどれか。
ア．各スレッドは必ず独立した仮想アドレス空間を持つ。
イ．一つのプロセスにはスレッドを一つしか作成できない。
ウ．スレッドはCPUを使用せず、入出力処理だけを行う。
エ．同一プロセス内の複数スレッドは、一般にアドレス空間などの資源を共有する。

正答・4肢解説・総合解説

正答：エ．同一プロセス内の複数スレッドは、一般にアドレス空間などの資源を共有する。
ア：独立したアドレス空間を持つのは通常プロセス単位であり、同一プロセスのスレッドはアドレス空間を共有する。
イ：多くのOSでは一つのプロセス内に複数のスレッドを作成できる。
ウ：スレッドはCPU上で命令を実行するスケジューリング対象となり得る。
エ：スレッドは実行単位であり、同一プロセスに属するスレッドは多くの資源を共有するため、プロセス間通信より軽量に連携できる場合が多い。
総合解説：プロセスは資源の保護・分離の単位、スレッドはプロセス内の実行単位として理解すると整理しやすい。スレッド間の共有資源は利便性と同時に競合条件の原因にもなる。

Q003 1-1 IT基盤 / OS・ハードウェア

ページング方式の仮想記憶でページフォールトが発生するのは、どのような場合か。
ア．CPUのクロック周波数が一時的に低下した場合。
イ．同じファイルを二つのプロセスが同時に開いた場合。
ウ．ネットワークのTTLが0になった場合。
エ．参照しようとした仮想ページが主記憶上に存在せず、補助記憶などから読み込む必要がある場合。

正答・4肢解説・総合解説

正答：エ．参照しようとした仮想ページが主記憶上に存在せず、補助記憶などから読み込む必要がある場合。
ア：クロック周波数の変化はページフォールトの直接原因ではない。
イ：ファイル共有の有無だけでページフォールトが発生するわけではない。
ウ：TTLはIPパケットの寿命に関する値であり、仮想記憶とは無関係である。
エ：ページフォールトは、参照対象ページが主記憶にないときに発生し、OSが必要なページを読み込む処理を行う。
総合解説：仮想記憶は主記憶より大きなアドレス空間を扱いやすくする一方、ページイン・ページアウトが頻発すると性能が大きく低下する。

Q004 1-1 IT基盤 / OS・ハードウェア

OSがユーザモードとカーネルモードを分ける主な目的として、最も適切なものはどれか。
ア．ユーザモードのプログラムだけCPUキャッシュを利用できるようにするため。
イ．カーネルモードではネットワーク通信を禁止するため。
ウ．特権命令や重要なハードウェア資源への直接アクセスを制限し、システム全体を保護するため。
エ．アプリケーションごとにCPUの物理個数を変えるため。

正答・4肢解説・総合解説

正答：ウ．特権命令や重要なハードウェア資源への直接アクセスを制限し、システム全体を保護するため。
ア：CPUキャッシュの利用をユーザモードだけに限定する仕組みではない。
イ：カーネルはネットワーク処理を含む多くの低レベル処理を担う。
ウ：モード分離により、一般アプリケーションが無制限に特権命令を実行することを防ぎ、障害や不正操作の影響を抑える。
エ：モード分離の目的はCPU個数の変更ではなく、権限と保護境界の確立である。
総合解説：特権分離はOSセキュリティの基礎である。アプリケーションはシステムコールなどの制御された経路を通じてOS機能を利用する。

Q005 1-1 IT基盤 / OS・ハードウェア

CPUキャッシュメモリの主な目的はどれか。
ア．停電時でも主記憶の内容を永久保存する。
イ．ネットワーク上のIPアドレスをMACアドレスに変換する。
ウ．CPUと主記憶の速度差を緩和し、頻繁に使うデータや命令へのアクセスを高速化する。
エ．ファイルを暗号化して機密性を保証する。

正答・4肢解説・総合解説

正答：ウ．CPUと主記憶の速度差を緩和し、頻繁に使うデータや命令へのアクセスを高速化する。
ア：キャッシュは通常揮発性であり、永続保存を目的としない。
イ：これはARPの役割であり、CPUキャッシュとは無関係である。
ウ：キャッシュは局所性を利用し、主記憶より高速な記憶領域に頻繁に参照されるデータを保持する。
エ：キャッシュの主目的は性能向上であり、暗号化機能ではない。
総合解説：CPU性能は演算速度だけでなく、メモリアクセス待ちの影響を大きく受ける。キャッシュはこの待ち時間を減らすための重要な構成要素である。

Q006 1-1 IT基盤 / OS・ハードウェア

2台の同容量ディスクを用いたRAID 1の特徴として、最も適切なものはどれか。
ア．データをブロック単位で分散するだけで、冗長情報は持たない。
イ．3台以上のディスクに分散パリティを必ず保存する。
ウ．ディスク故障時でもバックアップが不要になる。
エ．同じデータを複数ディスクに複製するミラーリングにより、1台の故障に耐えられる構成が可能である。

正答・4肢解説・総合解説

正答：エ．同じデータを複数ディスクに複製するミラーリングにより、1台の故障に耐えられる構成が可能である。
ア：これはRAID 0の代表的な考え方であり、冗長性を持たない。
イ：分散パリティはRAID 5の特徴であり、RAID 1の必須要件ではない。
ウ：RAIDは可用性向上策であり、誤削除やランサムウェア等に備えるバックアップの代替にはならない。
エ：RAID 1は同一内容を複数ディスクに保持するため、一般にディスク単体故障への可用性を高められる。
総合解説：RAIDは可用性向上の技術であり、バックアップとは目的が異なる。ミラーリングでも論理破壊や誤削除は複製され得る。

Q007 1-1 IT基盤 / OS・ハードウェア

宇宙線などによる一時的なビット反転が問題となるサーバで、メモリ上の単一ビット誤りの検出・訂正能力を高めたい。適した技術はどれか。
ア．CPUキャッシュを無効化する。
イ．ECCメモリを採用する。
ウ．DNSSECを有効化する。
エ．データベースの正規化を行う。

正答・4肢解説・総合解説

正答：イ．ECCメモリを採用する。
ア：キャッシュ無効化は性能に影響し、メモリのビット誤り訂正手段にはならない。
イ：ECCメモリは誤り訂正符号を用いて、一定範囲のビット誤りを検出・訂正できるため、信頼性が重要なサーバで利用される。
ウ：DNSSECはDNS応答の真正性・完全性を検証する仕組みであり、主記憶の誤り訂正とは無関係である。
エ：正規化はデータ構造の冗長性や更新異常を抑える設計手法であり、物理メモリのビット誤り対策ではない。
総合解説：ハードウェア故障や一時的ビット誤りも可用性・完全性に影響する。セキュリティではソフトウェアだけでなく基盤の信頼性も考慮する。

Q008 1-1 IT基盤 / OS・ハードウェア

ハードウェア割込みの説明として、最も適切なものはどれか。
ア．CPUが必ず電源を切るための信号である。
イ．入出力完了などの事象をCPUへ通知し、CPUが現在の処理を一時中断して割込み処理を実行できるようにする。
ウ．主記憶の内容を自動的に暗号化する機能である。
エ．IPパケットの送信先を変更する仕組みである。

正答・4肢解説・総合解説

正答：イ．入出力完了などの事象をCPUへ通知し、CPUが現在の処理を一時中断して割込み処理を実行できるようにする。
ア：割込みは多様なイベント通知に使われ、電源断だけを意味しない。
イ：割込みにより、CPUは周辺装置を常時ポーリングせずに、必要なタイミングでイベントを処理できる。
ウ：割込みは制御機構であり、暗号化機能そのものではない。
エ：パケット転送先の判断はルーティング等の機能であり、割込みの説明ではない。
総合解説：割込み発生時には実行状態の退避と復帰が必要であり、OSのデバイス制御やスケジューリングと密接に関係する。

Q009 1-1 IT基盤 / OS・ハードウェア

DMA（Direct Memory Access）の特徴として、最も適切なものはどれか。
ア．CPUを使わずにアプリケーションの命令そのものを実行する。
イ．入出力装置と主記憶の間のデータ転送を、CPUが1バイトずつ処理せずに行える。
ウ．インターネット上の経路選択を自動化する。
エ．パスワードをハッシュ化して保存する。

正答・4肢解説・総合解説

正答：イ．入出力装置と主記憶の間のデータ転送を、CPUが1バイトずつ処理せずに行える。
ア：DMAは主にデータ転送の仕組みであり、一般のアプリケーション命令を代行実行するものではない。
イ：DMAはデータ転送の負荷を専用機構に任せ、CPUの関与を減らすことで効率を高める。
ウ：経路選択はルーティングの役割であり、DMAとは無関係である。
エ：DMAはメモリ転送技術であり、パスワード保護技術ではない。
総合解説：DMAはI/O性能を高める重要な仕組みである一方、セキュリティ設計ではDMA可能なデバイスからのメモリアクセス制御も考慮対象となる。

Q010 1-1 IT基盤 / OS・ハードウェア

Secure Bootの主な目的として、最も適切なものはどれか。
ア．起動後の全通信を自動的にVPNへ切り替える。
イ．起動時に署名などを検証し、信頼されていないブートローダや低レベルコードの実行を抑止する。
ウ．主記憶容量を仮想的に増やす。
エ．データベースのトランザクションを直列化する。

正答・4肢解説・総合解説

正答：イ．起動時に署名などを検証し、信頼されていないブートローダや低レベルコードの実行を抑止する。
ア：Secure Bootは起動時の信頼性検証が中心で、VPN接続制御そのものではない。
イ：Secure Bootは起動チェーンの信頼性を検証し、OS起動前に不正コードが実行されるリスクを低減する。
ウ：これは仮想記憶の役割であり、Secure Bootとは異なる。
エ：これはDBの同時実行制御に関する処理で、起動時検証とは無関係である。
総合解説：Secure Bootは信頼の起点から起動コンポーネントを検証する考え方であり、ブートキット等への対策の一部となる。

Q011 1-1 IT基盤 / OS・ハードウェア

一般にType 1ハイパーバイザの説明として、最も適切なものはどれか。
ア．通常のホストOS上のアプリケーションとしてのみ動作する。
イ．仮想マシン同士で必ず同一のOSカーネルを共有する。
ウ．物理CPUを一切使用せずに仮想CPUを実現する。
エ．ホストOSを介さず、物理ハードウェア上で直接動作するハイパーバイザである。

正答・4肢解説・総合解説

正答：エ．ホストOSを介さず、物理ハードウェア上で直接動作するハイパーバイザである。
ア：これはType 2（ホスト型）ハイパーバイザの説明に近い。
イ：同一カーネル共有はコンテナの特徴であり、仮想マシンでは各ゲストOSが独自カーネルを持てる。
ウ：仮想CPUも最終的には物理CPU資源を利用する。
エ：Type 1はベアメタル型とも呼ばれ、物理基盤上で直接仮想マシンを管理する。
総合解説：仮想化方式の違いは分離境界や管理面の設計に関係する。クラウド基盤のセキュリティを考える際も、ハイパーバイザとゲストOSの責任範囲を区別する。

Q012 1-1 IT基盤 / OS・ハードウェア

あるOSで、アプリケーションAの不具合により任意アドレスへ書込みが発生した。Aが別プロセスBのメモリを書き換える被害を抑える上で、最も直接的なOS機構はどれか。
ア．DNSキャッシュの保持時間を短くする。
イ．プロセスごとの仮想アドレス空間とページ単位のアクセス権によるメモリ保護。
ウ．RAID 1でディスクをミラーリングする。
エ．DHCPのリース時間を長くする。

正答・4肢解説・総合解説

正答：イ．プロセスごとの仮想アドレス空間とページ単位のアクセス権によるメモリ保護。
ア：DNSキャッシュ設定は名前解決に関するもので、プロセスメモリ分離には効果がない。
イ：プロセス分離とページ保護により、通常は他プロセスのメモリへ直接読み書きできないよう制御する。
ウ：RAID 1は記憶装置の可用性向上策であり、メモリアクセス違反を防ぐものではない。
エ：DHCPリース時間はIP設定の保持期間であり、メモリ保護とは無関係である。
総合解説：OSの保護境界は、単一アプリケーションの障害や侵害が他のプロセスへ波及するのを抑える基本要素である。ただしカーネル侵害などではこの境界自体が破られる可能性がある。

Q013 1-1 IT基盤 / ネットワーク基礎

TCPの特徴として、UDPと比較して最も適切なものはどれか。
ア．常に暗号化された通信を提供する。
イ．コネクションを確立し、順序制御や再送制御によって信頼性のあるバイトストリームを提供する。
ウ．IPアドレスをMACアドレスへ変換する。
エ．名前をIPアドレスへ変換する。

正答・4肢解説・総合解説

正答：イ．コネクションを確立し、順序制御や再送制御によって信頼性のあるバイトストリームを提供する。
ア：TCP自体は暗号化を必須としない。暗号化にはTLS等の上位層の仕組みが必要である。
イ：TCPは接続管理、順序番号、確認応答、再送などを用いて信頼性を提供する。
ウ：これはARPの役割であり、TCPの機能ではない。
エ：これはDNSの代表的な役割であり、TCPの機能ではない。
総合解説：TCPとUDPは用途に応じて使い分ける。信頼性や順序制御が必要ならTCPが適する場合が多く、低遅延やアプリケーション側制御を重視する場合にはUDPが使われる。

Q014 1-1 IT基盤 / ネットワーク基礎

TCPの3ウェイハンドシェイクの基本的な順序として、正しいものはどれか。
ア．ACK → SYN → FIN
イ．SYN → SYN/ACK → ACK
ウ．FIN → ACK → SYN
エ．ARP → DNS → ACK

正答・4肢解説・総合解説

正答：イ．SYN → SYN/ACK → ACK
ア：接続開始時はSYNから始まり、この順序ではない。
イ：クライアントのSYNに対しサーバがSYN/ACKを返し、最後にクライアントがACKを返すのが基本形である。
ウ：FINは主に接続終了処理で使われ、接続確立の開始ではない。
エ：ARPやDNSは別のプロトコルであり、TCPハンドシェイクのメッセージではない。
総合解説：TCP接続管理を理解すると、SYN floodなどの攻撃や状態追跡型ファイアウォールの挙動も理解しやすくなる。

Q015 1-1 IT基盤 / ネットワーク基礎

一般的なIPv4サブネット192.0.2.0/26で、ネットワークアドレスとブロードキャストアドレスを除いた利用可能なホストアドレス数はいくつか。
ア．30（/27相当の利用可能ホスト数）
イ．64（/26の総アドレス数）
ウ．126（/25相当の利用可能ホスト数）
エ．62（64個からネットワークアドレスとブロードキャストアドレスを除いた数）

正答・4肢解説・総合解説

正答：エ．62（64個からネットワークアドレスとブロードキャストアドレスを除いた数）
ア：30は/27の32個から予約2個を除いた利用可能ホスト数であり、/26ではない。
イ：/26の総アドレス数は64個だが、ネットワークアドレスとブロードキャストアドレスは通常ホストへ割り当てない。
ウ：126は/25の128個から予約2個を除いた利用可能ホスト数であり、/26ではない。
エ：/26は64個のアドレスを持ち、ネットワークアドレスとブロードキャストアドレスを除くと利用可能なホストアドレスは62個である。
総合解説：CIDR表記からホスト部のビット数を求め、2のべき乗で総アドレス数を計算する。試験では例外的な用途ではなく、一般的なサブネットとして問われることが多い。

Q016 1-1 IT基盤 / ネットワーク基礎

IPv4の同一LAN内で、送信先IPアドレスに対応するMACアドレスを求めるために用いられる代表的なプロトコルはどれか。
ア．DNS
イ．ARP
ウ．DHCP
エ．SMTP

正答・4肢解説・総合解説

正答：イ．ARP
ア：DNSは主にドメイン名とIPアドレスなどの情報を対応付ける。
イ：ARPはIPv4アドレスとリンク層のMACアドレスの対応を解決するために用いられる。
ウ：DHCPはIPアドレスやゲートウェイ、DNSサーバ等の設定を自動配布する。
エ：SMTPは電子メール送信に用いられるアプリケーション層プロトコルである。
総合解説：ARPはローカルネットワークで重要な役割を持つ一方、ARP spoofingなどの攻撃対象にもなる。

Q017 1-1 IT基盤 / ネットワーク基礎

DNSの主な役割として、最も適切なものはどれか。
ア．LAN内の端末へIPアドレスを自動割り当てする。
イ．IPパケットを暗号化してVPNを確立する。
ウ．ドメイン名とIPアドレスなどのDNSリソース情報を対応付け、名前解決を行う。
エ．同一LAN内でIPアドレスからMACアドレスを求める。

正答・4肢解説・総合解説

正答：ウ．ドメイン名とIPアドレスなどのDNSリソース情報を対応付け、名前解決を行う。
ア：これはDHCPの役割であり、DNSの名前解決機能とは異なる。
イ：VPN暗号化はIPsecやTLS等の仕組みで行われ、DNSの基本機能ではない。
ウ：DNSは階層的な名前空間を用いて、ホスト名等からIPアドレスなどの情報を検索できるようにする。
エ：これはARPの役割であり、TCPの機能ではない。
総合解説：DNSはインターネットの基盤サービスであり、可用性や応答の真正性が損なわれると広範な影響が生じる。

Q018 1-1 IT基盤 / ネットワーク基礎

新しいPCを社内LANへ接続したところ、管理者が手入力しなくてもIPアドレス、サブネットマスク、デフォルトゲートウェイ等が設定された。主に利用された仕組みはどれか。
ア．DHCP
イ．ARP
ウ．NTP
エ．SNMP

正答・4肢解説・総合解説

正答：ア．DHCP
ア：DHCPはクライアントへネットワーク設定を自動配布するために用いられる。
イ：ARPはIPアドレスに対応するMACアドレスの解決に使う。
ウ：NTPは機器間の時刻同期に用いるプロトコルであり、IP設定の自動配布は行わない。
エ：SNMPはネットワーク機器等の監視・管理に利用される。
総合解説：DHCPは運用を簡素化するが、不正DHCPサーバによる誤設定配布などのリスクもある。ネットワーク基礎とセキュリティは切り離せない。

Q019 1-1 IT基盤 / ネットワーク基礎

ルータの主な役割として、最も適切なものはどれか。
ア．異なるIPネットワーク間で、ルーティング情報に基づいてパケットを転送する。
イ．アプリケーションのソースコードをコンパイルする。
ウ．データベースの行ロックを管理する。
エ．利用者のパスワードを必ず多要素認証へ変換する。

正答・4肢解説・総合解説

正答：ア．異なるIPネットワーク間で、ルーティング情報に基づいてパケットを転送する。
ア：ルータはIP層で宛先ネットワークを判断し、次ホップなどを選択してパケットを転送する。
イ：コンパイルは開発ツールの役割であり、ルータの機能ではない。
ウ：行ロックはDBMSの同時実行制御に関する機能である。
エ：認証方式の管理はIAM等の領域であり、ルーター般の基本役割ではない。
総合解説：ルーティングはネットワーク到達性の基礎であり、誤設定や不正な経路情報は通信の可用性・機密性に影響する。

Q020 1-1 IT基盤 / ネットワーク基礎

NATの説明として、最も適切なものはどれか。
ア．NATを導入すれば、ファイアウォールのアクセス制御は常に不要になる。
イ．NATはDNS応答に必ずデジタル署名を付ける。
ウ．IPアドレスやポート番号を変換して、内部ネットワークと外部ネットワークの通信を成立させるために用いられる。
エ．NATはTCPだけで利用でき、UDPでは利用できない。

正答・4肢解説・総合解説

正答：ウ．IPアドレスやポート番号を変換して、内部ネットワークと外部ネットワークの通信を成立させるために用いられる。
ア：NATは変換機能であり、セキュリティポリシーに基づく通信許可・拒否を代替するものではない。
イ：DNS応答の署名はDNSSECに関する機能であり、NATの役割ではない。
ウ：NATはアドレス変換機能であり、プライベートアドレスの端末から外部へ通信する際などに使われる。
エ：NAT/NAPTはUDP通信でも利用される。
総合解説：NATには副次的に内部アドレスを直接露出しにくくする効果があるが、それだけで十分なセキュリティ境界とはならない。

Q021 1-1 IT基盤 / ネットワーク基礎

端末Aが、自身と異なるIPv4サブネットにある端末Bへパケットを送る。端末Aで通常最初に参照される設定として最も適切なものはどれか。
ア．CPUキャッシュサイズ
イ．データベースの主キー
ウ．ファイルシステムのマウントポイント
エ．デフォルトゲートウェイ

正答・4肢解説・総合解説

正答：エ．デフォルトゲートウェイ
ア：CPUキャッシュはネットワーク転送先の決定には使われない。
イ：主キーはDBレコード識別に用いるもので、IP転送経路とは無関係である。
ウ：マウントポイントはストレージ管理の概念であり、IP経路選択とは関係しない。
エ：宛先が同一サブネットにない場合、端末は通常ルーティングテーブルに従ってルータへ送信し、該当経路がなければデフォルトゲートウェイを利用する。
総合解説：端末は宛先IPとサブネットマスクから同一ネットワークかを判断し、異なる場合はルータへ渡す。ネットワーク障害の切り分けでも重要な基本である。

Q022 1-1 IT基盤 / ネットワーク基礎

IPパケットがルーティングループによってネットワーク内を無限に巡回することを防ぐための仕組みとして、最も適切なものはどれか。
ア．TCPのウィンドウサイズを必ず0にする。
イ．DNSキャッシュを毎回削除する。
ウ．MACアドレスを毎ホップでランダム化する。
エ．IPv4のTTL（IPv6ではHop Limit）を中継ごとに減少させ、0になったパケットを破棄する。

正答・4肢解説・総合解説

正答：エ．IPv4のTTL（IPv6ではHop Limit）を中継ごとに減少させ、0になったパケットを破棄する。
ア：ウィンドウサイズはフロー制御に関する値であり、IPループ防止の仕組みではない。
イ：DNSキャッシュの削除はルーティングループ防止にはならない。
ウ：MACアドレスをランダム化してもIP層のルーティングループは解消しない。
エ：TTL/Hop Limitはパケットの生存可能な中継回数を制限し、ループ時の無限転送を防ぐ。
総合解説：TTL/Hop Limitは障害時の被害拡大を抑える基本機構である。traceroute系の診断もこの性質を利用する。

Q023 1-1 IT基盤 / データベース・クラウド

データベーストランザクションのACID特性におけるAtomicity（原子性）の説明として、最も適切なものはどれか。
ア．複数の利用者が同じパスワードを使える性質。
イ．データを必ず複数の国に分散保存する性質。
ウ．検索結果を常に暗号化する性質。
エ．一連の処理をすべて実行するか、失敗時にはすべて取り消すかのいずれかとして扱う性質。

正答・4肢解説・総合解説

正答：エ．一連の処理をすべて実行するか、失敗時にはすべて取り消すかのいずれかとして扱う性質。
ア：認証に関する説明であり、ACIDの原子性ではない。
イ：地理的冗長化は可用性設計の一つであり、原子性の定義ではない。
ウ：暗号化は機密性対策であり、原子性とは異なる。
エ：原子性はトランザクション途中の一部だけが確定することを避け、処理単位の整合性を保つ。
総合解説：ACIDはトランザクション処理の重要な基礎である。原子性、整合性、一貫した分離、永続性を区別して理解する。

Q024 1-1 IT基盤 / データベース・クラウド

関係データベースの正規化を行う主な目的として、最も適切なものはどれか。
ア．データの冗長性を抑え、挿入・更新・削除時の不整合を起こしにくくする。
イ．全ての表を一つの巨大な表へ統合する。
ウ．全ての列を暗号化する。
エ．SQL文の実行権限を全利用者へ付与する。

正答・4肢解説・総合解説

正答：ア．データの冗長性を抑え、挿入・更新・削除時の不整合を起こしにくくする。
ア：正規化は属性間の依存関係を整理し、重複データや更新異常を減らすための設計手法である。
イ：正規化はむしろ適切な関係に分解することが多い。
ウ：暗号化は機密性対策であり、正規化の目的ではない。
エ：これはアクセス制御の問題であり、正規化とは無関係である。
総合解説：正規化はデータモデルの整合性向上に役立つが、性能要件によっては意図的な非正規化を検討する場合もある。

Q025 1-1 IT基盤 / データベース・クラウド

データベースのインデックスに関する説明として、最も適切なものはどれか。
ア．インデックスを作れば、全てのSQLが必ず高速化する。
イ．インデックスはバックアップの代替である。
ウ．検索を高速化できる場合がある一方、追加の記憶領域や更新時の保守コストが発生する。
エ．インデックスを作るとアクセス制御が不要になる。

正答・4肢解説・総合解説

正答：ウ．検索を高速化できる場合がある一方、追加の記憶領域や更新時の保守コストが発生する。
ア：検索条件やデータ分布によって効果は異なり、更新処理では負荷が増えることもある。
イ：インデックスは検索構造であり、障害復旧用バックアップの代わりにはならない。
ウ：インデックスは特定条件の検索を効率化するが、INSERTやUPDATE時にはインデックス更新が必要になる。
エ：検索性能とアクセス制御は別の問題である。
総合解説：インデックスは性能設計の代表的なトレードオフである。セキュリティ監視用ログDBでも、検索性能と書込み負荷の両方を考える必要がある。

Q026 1-1 IT基盤 / データベース・クラウド

データベースのトランザクション分離（Isolation）の主な目的として、最も適切なものはどれか。
ア．データベースサーバの電源を二重化する。
イ．利用者のパスワードを公開鍵で配布する。
ウ．並行実行されるトランザクション同士の不適切な干渉を抑える。
エ．DNSの名前解決結果をキャッシュする。

正答・4肢解説・総合解説

正答：ウ．並行実行されるトランザクション同士の不適切な干渉を抑える。
ア：これは可用性向上策であり、トランザクション分離ではない。
イ：認証・鍵管理の話であり、トランザクション分離とは無関係である。
ウ：分離レベルは、ダーティリードなどの並行実行時の不整合をどこまで許容するかと性能のバランスに関係する。
エ：DNSキャッシュはネットワークサービスの機能である。
総合解説：同時実行制御はデータ完全性に直結する。分離レベルを強くすると整合性を高めやすい一方、並行性が下がる場合がある。

Q027 1-1 IT基盤 / データベース・クラウド

一般的なIaaSを利用し、クラウド事業者が物理設備と仮想化基盤を提供し、利用者が仮想マシン上のOSとアプリケーションを管理している。この場合、利用者側の責任として最も適切なものはどれか。
ア．クラウド事業者のデータセンタ建屋の電源設備を保守する。
イ．ハイパーバイザ製品の物理ホストへの導入を利用者が必ず行う。
ウ．ゲストOSのパッチ適用やアプリケーション設定、アカウント管理を行う。
エ．クラウド事業者の従業員の採用審査を利用者が実施する。

正答・4肢解説・総合解説

正答：ウ．ゲストOSのパッチ適用やアプリケーション設定、アカウント管理を行う。
ア：通常、物理データセンタ設備はクラウド事業者の責任範囲である。
イ：一般的なIaaSでは基盤ハイパーバイザは事業者が管理する。
ウ：IaaSではクラウド事業者が物理基盤等を管理する一方、利用者はゲストOSやアプリケーション、データ、IAM設定など多くの責任を持つ。
エ：事業者組織の人事管理は通常利用者の責任ではない。
総合解説：クラウドのセキュリティは「利用すれば任せられる」のではなく、サービスモデルごとに責任分界を確認することが重要である。

Q028 1-1 IT基盤 / データベース・クラウド

SaaSの一般的な特徴として、最も適切なものはどれか。
ア．利用者が必ず物理サーバを購入してデータセンタへ設置する。
イ．利用者が必ずハイパーバイザを直接管理する。
ウ．利用者は完成したアプリケーションをサービスとして利用し、基盤やアプリケーション本体の運用は主に事業者が担う。
エ．利用者は認証設定やデータ公開範囲について一切責任を負わない。

正答・4肢解説・総合解説

正答：ウ．利用者は完成したアプリケーションをサービスとして利用し、基盤やアプリケーション本体の運用は主に事業者が担う。
ア：これはSaaSの一般的な利用形態ではない。
イ：SaaSでは通常ハイパーバイザは事業者側の管理範囲である。
ウ：SaaSではインフラからアプリケーションまで事業者側が広く管理する一方、利用者はアカウント、データ利用、設定等の責任を引き続き持つ。
エ：SaaSでも利用者側設定やアカウント管理が原因で情報漏えいする可能性があり、責任は残る。
総合解説：SaaSは運用負担を減らせるが、ID管理、データ分類、共有設定、監査ログの確認など利用者側の管理が不要になるわけではない。

Q029 1-1 IT基盤 / データベース・クラウド

一般的なOSレベルのコンテナと仮想マシンの違いとして、最も適切なものはどれか。
ア．コンテナは通常ホストOSのカーネルを共有し、仮想マシンはゲストOSごとに独自のカーネルを持てる。
イ．コンテナはCPUを使用せず、仮想マシンだけがCPUを使用する。
ウ．仮想マシンはネットワーク接続できない。
エ．コンテナではアクセス制御や脆弱性管理が不要である。

正答・4肢解説・総合解説

正答：ア．コンテナは通常ホストOSのカーネルを共有し、仮想マシンはゲストOSごとに独自のカーネルを持てる。
ア：コンテナはプロセス分離を活用して軽量に実行できる一方、仮想マシンはハイパーバイザ上でゲストOSを動かす。
イ：どちらも最終的には物理CPU資源を利用する。
ウ：仮想NIC等を通じてネットワーク接続できる。
エ：コンテナにもイメージ、実行権限、脆弱性、設定などのセキュリティ管理が必要である。
総合解説：コンテナと仮想マシンでは分離境界が異なる。設計時にはホストカーネル侵害時の影響やイメージ管理などを考慮する。

Q030 1-1 IT基盤 / データベース・クラウド

クラウド利用企業が「クラウド事業者がISO認証を持っているので、自社側のアクセス権設定ミスはセキュリティ問題にならない」と主張した。最も適切な評価はどれか。
ア．不適切である。クラウド事業者の管理策と利用者側の設定責任は別であり、利用者の誤設定は事故原因になり得る。
イ．適切である。クラウドを使えば利用者のセキュリティ責任は全て事業者へ移転する。
ウ．適切である。アクセス権は性能だけに影響し、機密性には影響しない。
エ．不適切であるが、理由はクラウドではアクセス制御を利用できないからである。

正答・4肢解説・総合解説

正答：ア．不適切である。クラウド事業者の管理策と利用者側の設定責任は別であり、利用者の誤設定は事故原因になり得る。
ア：クラウドではサービスモデルや契約に応じた責任分界があり、認証取得や事業者側管理策だけで利用者側責任が消えるわけではない。
イ：クラウドでも利用者側のID、データ、設定などの責任は残る。
ウ：アクセス権の誤設定は不正閲覧や漏えいに直結し、機密性へ影響する。
エ：クラウドでもIAM等のアクセス制御は一般に利用できる。問題は適切に設定・運用する責任である。
総合解説：クラウドセキュリティでは、事業者の認証・監査結果だけでなく、自組織の責任範囲、設定、運用、ログ確認を明確にする必要がある。

Q031 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

情報セキュリティにおける機密性（Confidentiality）の説明として、最も適切なものはどれか。
ア．情報が正確で完全な状態を維持する特性。
イ．認可されていない個人、主体又はプロセスに情報を開示しないよう保護する特性。
ウ．必要なときに情報へアクセスできる特性。
エ．処理速度を常に最大化する特性。

正答・4肢解説・総合解説

正答：イ．認可されていない個人、主体又はプロセスに情報を開示しないよう保護する特性。
ア：これは主に完全性の説明であり、機密性の定義ではない。
イ：機密性は情報が許可された主体だけに開示・利用される状態を守る考え方である。
ウ：これは可用性の説明であり、機密性の定義ではない。
エ：性能は重要だがCIAの機密性の定義ではない。
総合解説：CIAは情報セキュリティの基本3要素である。対策の目的が機密性・完全性・可用性のどれに主に効くかを区別する。

Q032 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

情報セキュリティにおける完全性（Integrity）の説明として、最も適切なものはどれか。
ア．情報を誰にも開示しない特性。
イ．サービスを24時間365日必ず停止させない特性。
ウ．利用者の本人確認だけを行う特性。
エ．情報や処理が不正又は不適切に変更・破壊されず、正確さと完全さが保たれる特性。

正答・4肢解説・総合解説

正答：エ．情報や処理が不正又は不適切に変更・破壊されず、正確さと完全さが保たれる特性。
ア：機密性は認可された主体には利用を許すため、誰にも開示しないことが定義ではない。
イ：可用性に関連するが、絶対無停止を意味するわけではなく、完全性の説明でもない。
ウ：本人確認は認証に関する機能であり、完全性そのものではない。
エ：完全性は情報の無断改ざんや誤った変更を防ぎ、正確性・完全性を維持する考え方である。
総合解説：改ざん検知、適切な権限管理、トランザクション制御などは完全性維持に寄与する。

Q033 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

情報セキュリティにおける可用性（Availability）の説明として、最も適切なものはどれか。
ア．認可された利用者が必要なときに情報やシステムを利用できる特性。
イ．全ての情報を公開する特性。
ウ．情報を変更できる利用者を増やす特性。
エ．全ログを暗号化すれば自動的に満たされる特性。

正答・4肢解説・総合解説

正答：ア．認可された利用者が必要なときに情報やシステムを利用できる特性。
ア：可用性は必要なサービスや情報が適時に利用できる状態を維持することを指す。
イ：公開範囲の拡大は可用性の定義ではなく、機密性を損なう場合がある。
ウ：変更権限の増加は完全性リスクを高める可能性があり、可用性の定義ではない。
エ：暗号化は主に機密性に寄与し、可用性を自動的に保証しない。
総合解説：冗長化、バックアップ、容量管理、DDoS対策、災害対策などは可用性を高める代表例である。

Q034 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

脅威と脆弱性の関係として、最も適切なものはどれか。
ア．脅威と脆弱性は常に同じ意味である。
イ．脅威は損害を生じさせ得る原因・事象であり、脆弱性は脅威によって悪用され得る弱点である。
ウ．脆弱性は攻撃者そのものを意味する。
エ．脅威は必ずソフトウェアのバグだけを指す。

正答・4肢解説・総合解説

正答：イ．脅威は損害を生じさせ得る原因・事象であり、脆弱性は脅威によって悪用され得る弱点である。
ア：両者は異なる概念であり、リスク分析では区別する必要がある。
イ：リスクを考える際は、守る対象、脅威、脆弱性、影響を関連付けて整理する。
ウ：攻撃者は脅威源の一例であり、脆弱性は弱点を指す。
エ：自然災害、人為ミス、故障、攻撃者など多様な脅威がある。
総合解説：「公開サーバに未修正の欠陥がある」は脆弱性、「攻撃者がその欠陥を悪用する」は脅威シナリオの一部、と整理できる。

Q035 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

情報セキュリティリスクの説明として、最も適切なものはどれか。
ア．脆弱性が一つでもあれば、必ず同じ大きさのリスクになる。
イ．攻撃が実際に発生した後だけをリスクと呼ぶ。
ウ．リスクはIT機器の購入価格だけで決まる。
エ．脅威が脆弱性などを通じて情報資産へ影響を及ぼす可能性と、その結果の重大さを考慮して評価する。

正答・4肢解説・総合解説

正答：エ．脅威が脆弱性などを通じて情報資産へ影響を及ぼす可能性と、その結果の重大さを考慮して評価する。
ア：脆弱性の悪用可能性、資産価値、影響、既存管理策などによりリスクは変わる。
イ：リスクは将来の不確実な事象も含めて評価する概念である。
ウ：金銭価値以外に業務停止、法的影響、信用低下等も考慮し得る。
エ：リスクは単なる弱点の有無ではなく、発生可能性や影響、組織のリスク基準を踏まえて評価する。
総合解説：リスク評価では、技術的な深刻度だけでなく組織への事業影響を結び付けて判断することが重要である。

Q036 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

「Webサーバに既知の脆弱性が存在するが、悪用された証拠は確認されていない」という状況の説明として、最も適切なものはどれか。
ア．脆弱性は存在するが、それだけでセキュリティインシデントが発生したと断定はできない。
イ．脆弱性があれば必ず侵害済みである。
ウ．悪用されていなければ脆弱性ではない。
エ．脆弱性は物理設備にしか存在しない。

正答・4肢解説・総合解説

正答：ア．脆弱性は存在するが、それだけでセキュリティインシデントが発生したと断定はできない。
ア：脆弱性は弱点であり、インシデントはセキュリティを損なう事象である。脆弱性の存在と侵害の発生は区別する。
イ：脆弱性が未悪用の可能性もあり、侵害の有無は証拠に基づき確認する必要がある。
ウ：悪用の有無にかかわらず、悪用され得る弱点は脆弱性である。
エ：ソフトウェア、設定、運用、人、物理設備など様々な弱点が脆弱性となり得る。
総合解説：脆弱性管理とインシデント対応は関連するが別の活動である。検知情報と脆弱性情報を組み合わせて優先度を判断する。

Q037 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

情報セキュリティの特性としての真正性（Authenticity）に最も近い説明はどれか。
ア．情報を常に公開状態にする性質。
イ．処理時間を短縮する性質。
ウ．障害発生時に必ず自動復旧する性質。
エ．主体や情報が、主張どおりのものであることを確認できる性質。

正答・4肢解説・総合解説

正答：エ．主体や情報が、主張どおりのものであることを確認できる性質。
ア：情報を公開することは真正性の定義ではなく、主体や情報が本物かどうかとは別問題である。
イ：処理性能は性能特性であり、主体や情報の真正性とは異なる概念である。
ウ：自動復旧は可用性向上策の一つであり、真正性の定義ではない。
エ：真正性は利用者、機器、情報などが本物であり、なりすましではないことを確かめられる性質に関係する。
総合解説：真正性は認証やデジタル署名、証明書などと関係が深い。CIAに加えて問われることがあるため区別する。

Q038 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

「誰が、いつ、どの管理操作を行ったかを後から確認できるよう、特権操作ログを利用者IDと時刻付きで保存する」対策が主に高める性質はどれか。
ア．可用性
イ．責任追跡性（Accountability）
ウ．圧縮率
エ．帯域幅

正答・4肢解説・総合解説

正答：イ．責任追跡性（Accountability）
ア：ログ保存は可用性にも間接的効果があるが、設問の中心は操作主体の追跡可能性である。
イ：操作主体と行為を追跡できる証拠を残すことで、行為の責任を特定しやすくする。
ウ：ログの記録は圧縮率を高めることが目的ではない。
エ：ネットワーク帯域幅は通信容量の指標であり、責任追跡性とは異なる。
総合解説：特権操作ログでは、改ざん防止、時刻同期、アクセス制限、保存期間なども重要である。

Q039 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

否認防止（Non-repudiation）の説明として、最も適切なものはどれか。
ア．障害時にサービスを継続する性質。
イ．情報を圧縮して保存容量を減らす性質。
ウ．ある行為やデータ送信を行った主体が、後からその事実を不当に否定しにくくする性質。
エ．全利用者へ同じ権限を与える性質。

正答・4肢解説・総合解説

正答：ウ．ある行為やデータ送信を行った主体が、後からその事実を不当に否定しにくくする性質。
ア：これは主に可用性に関係する説明であり、否認防止の定義ではない。
イ：圧縮は記憶効率の話で、否認防止とは関係しない。
ウ：デジタル署名や適切な監査証跡は、行為の証拠を残し否認防止に寄与する。
エ：権限均一化は否認防止の定義ではなく、最小権限にも反する可能性がある。
総合解説：否認防止は真正性・完全性・責任追跡性と関連するが同一概念ではない。どの証拠が誰の行為を裏付けるかを考える。

Q040 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

攻撃者が従業員になりすまし、電話でヘルプデスクに「緊急なのでパスワードをリセットしてほしい」と依頼して認証情報を得ようとした。この手口に最も該当するものはどれか。
ア．SQLインジェクション
イ．バッファオーバーフロー
ウ．ソーシャルエンジニアリング
エ．ルーティングプロトコルの収束

正答・4肢解説・総合解説

正答：ウ．ソーシャルエンジニアリング
ア：SQLインジェクションは入力値を通じて不正なSQLを実行させる技術的攻撃である。
イ：メモリ境界の不適切な処理を悪用する攻撃であり、電話でのなりすましとは異なる。
ウ：人の心理や手続上の隙を利用して情報や権限を得る手口はソーシャルエンジニアリングに該当する。
エ：これはネットワーク経路計算の挙動であり、攻撃手口の説明ではない。
総合解説：技術的対策だけでなく、本人確認手順、教育、承認プロセスなど人的・運用的管理策が必要である。

Q041 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

攻撃対象領域（Attack Surface）を小さくする施策として、最も適切なものはどれか。
ア．不要なサービスやポートを停止し、外部から到達可能な機能を必要最小限にする。
イ．不要な管理用ポートも含めて全ポートをインターネットへ公開する。
ウ．全利用者へ管理者権限を付与する。
エ．脆弱性情報の収集を停止する。

正答・4肢解説・総合解説

正答：ア．不要なサービスやポートを停止し、外部から到達可能な機能を必要最小限にする。
ア：公開機能や入口が減れば、攻撃者が試行できる経路を減らせるため、攻撃対象領域の縮小につながる。
イ：到達可能な入口が増え、攻撃対象領域を拡大させる。
ウ：権限を拡大し、侵害時の影響を大きくする。
エ：脆弱性を把握できなくなり、リスク管理を悪化させる。
総合解説：攻撃対象領域の縮小はハードニングの基本である。不要機能の削除、ネットワーク分離、管理IFの限定などを組み合わせる。

Q042 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

データセンタで商用電源が長時間停止し、UPSの保持時間を超えたためサーバが停止した。この事象の分類として最も適切なものはどれか。
ア．暗号鍵の衝突による機密性侵害
イ．SQL正規化不足による完全性侵害
ウ．物理的・環境的脅威による可用性への影響
エ．DNSキャッシュポイズニングによる真正性侵害

正答・4肢解説・総合解説

正答：ウ．物理的・環境的脅威による可用性への影響
ア：電源停止は物理・環境上の事象であり、暗号鍵の衝突を原因とするものではない。
イ：DB設計上の正規化と電源供給障害は別問題である。
ウ：電力供給の妨害や設備障害は、IPAシラバスでも物理的・環境的脅威として扱われる。
エ：DNS攻撃ではなく、物理的な電源障害である。
総合解説：サイバーセキュリティでは自然災害、火災、水、電源、通信障害なども脅威として評価する。

Q043 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

一般に「ゼロデイ脆弱性」と呼ばれる状況の説明として、最も適切なものはどれか。
ア．修正プログラムが提供される前など、十分な対策が整う前に悪用され得る未知又は未修正の脆弱性。
イ．既に修正済みで、全端末へパッチ適用も完了した脆弱性だけを指す。
ウ．攻撃者が0人である脆弱性を指す。
エ．可用性にだけ影響し、機密性や完全性には影響しない脆弱性を指す。

正答・4肢解説・総合解説

正答：ア．修正プログラムが提供される前など、十分な対策が整う前に悪用され得る未知又は未修正の脆弱性。
ア：ゼロデイ脆弱性では、パッチ未提供の期間に緩和策や監視強化などでリスクを抑える必要がある。
イ：既に修正と適用が完了した状態は、ゼロデイ脆弱性の概念とは逆である。
ウ：名称の「ゼロ」は攻撃者数を意味せず、対策猶予がほとんどない状況を示す表現である。
エ：影響するセキュリティ特性は脆弱性によって異なる。
総合解説：ゼロデイ対策では、攻撃対象領域の縮小、EDR等の挙動検知、ネットワーク分離、脅威情報収集など多層防御が重要になる。

Q044 1-2 セキュリティ基礎 / CIA・脅威・脆弱性

公開サーバに重大な脆弱性があり、インターネット上の攻撃者が悪用を試みている。ベンダの修正プログラムを適用して脆弱性を解消した場合の説明として、最も適切なものはどれか。
ア．攻撃者が存在する限り、リスクは必ず全く変わらない。
イ．パッチ適用すると脅威源そのものが消滅する。
ウ．パッチ適用は可用性にしか影響せず、攻撃成功確率には影響しない。
エ．脅威源が存在し続けても、悪用可能な脆弱性が減ることで当該リスクは低下し得る。

正答・4肢解説・総合解説

正答：エ．脅威源が存在し続けても、悪用可能な脆弱性が減ることで当該リスクは低下し得る。
ア：脆弱性を解消すれば攻撃成功の可能性を下げられるため、リスクは変化し得る。
イ：攻撃者という脅威源が消えるわけではない。
ウ：脆弱性の修正は悪用可能性を直接下げることがある。
エ：リスクは脅威だけで決まらず、脆弱性、影響、既存管理策などとの組合せで変化する。
総合解説：脅威、脆弱性、管理策、資産、影響を分けて考えると、どの対策がリスクのどの要素に効くか判断しやすい。

Q045 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

共通鍵暗号方式の基本的な特徴として、最も適切なものはどれか。
ア．暗号化鍵は誰にでも公開し、復号鍵だけを秘密にする。
イ．鍵を一切使用せずに機密性を実現する。
ウ．暗号化と復号に、当事者間で共有する同一又は対応する秘密鍵を用いる。
エ．ハッシュ値から元データを必ず復元できる。

正答・4肢解説・総合解説

正答：ウ．暗号化と復号に、当事者間で共有する同一又は対応する秘密鍵を用いる。
ア：これは公開鍵暗号の典型的な考え方である。
イ：共通鍵暗号でも鍵は必要であり、安全な鍵生成・配送・保管・更新が基本要素となる。
ウ：共通鍵暗号は高速なデータ暗号化に適する一方、鍵を安全に共有・管理する方法が重要となる。
エ：ハッシュは暗号化とは異なり、通常は一方向性を前提とする。
総合解説：大量データの暗号化には共通鍵方式が使われることが多く、公開鍵方式と組み合わせるハイブリッド暗号も一般的である。

Q046 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

公開鍵暗号方式の説明として、最も適切なものはどれか。
ア．公開鍵と秘密鍵は常に同じ値でなければならない。
イ．数学的に関連する公開鍵と秘密鍵のペアを用い、公開鍵は公開しても秘密鍵を秘匿する。
ウ．秘密鍵も公開鍵と同様に広く公開する。
エ．公開鍵暗号はデジタル署名には利用できない。

正答・4肢解説・総合解説

正答：イ．数学的に関連する公開鍵と秘密鍵のペアを用い、公開鍵は公開しても秘密鍵を秘匿する。
ア：公開鍵暗号は異なるが数学的に関連した鍵ペアを用いる。
イ：公開鍵暗号では、用途に応じて公開鍵で暗号化し秘密鍵で復号する、又は秘密鍵で署名し公開鍵で検証するなどの利用がある。
ウ：秘密鍵の漏えいはなりすましや復号につながるため厳重に保護する。
エ：公開鍵暗号技術はデジタル署名の基礎として利用される。
総合解説：公開鍵の真正性を保証するために証明書やPKIが用いられる。鍵そのものだけでなく「その公開鍵が誰のものか」が重要である。

Q047 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

暗号学的ハッシュ関数の利用目的として、最も適切なものはどれか。
ア．入力から固定長のダイジェストを生成し、データの変更検知などに利用する。
イ．元データを秘密鍵なしで必ず復号する。
ウ．ネットワークの経路を自動選択する。
エ．利用者の権限をロールへ自動割当てする。

正答・4肢解説・総合解説

正答：ア．入力から固定長のダイジェストを生成し、データの変更検知などに利用する。
ア：ハッシュ値はメッセージの要約値として利用され、完全性確認やデジタル署名処理などで重要な役割を持つ。
イ：ハッシュは復号を前提とする可逆暗号ではない。
ウ：ネットワーク経路の選択はルーティングの役割であり、ハッシュ関数の機能ではない。
エ：これはRBAC等のアクセス制御の領域であり、ハッシュ関数の機能ではない。
総合解説：ハッシュは暗号化と混同しやすい。暗号化は復号を前提とするが、ハッシュは通常元データへの逆変換を困難にする一方向性を利用する。

Q048 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

暗号学的ハッシュ関数の「衝突耐性」に最も近い説明はどれか。
ア．任意の入力から必ず異なる長さのハッシュ値を出す性質。
イ．ハッシュ値から元入力を高速に復元できる性質。
ウ．同じ入力でも毎回必ず異なるハッシュ値を返す性質。
エ．同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難である性質。

正答・4肢解説・総合解説

正答：エ．同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難である性質。
ア：一般的な暗号学的ハッシュは固定長出力を生成する。
イ：ハッシュ値から元入力を高速に復元できることは、一方向性を重視する暗号学的ハッシュの考え方と反する。
ウ：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。
エ：衝突耐性は、異なるデータが同じダイジェストになる組合せを意図的に見つけることへの耐性である。
総合解説：衝突耐性、第二原像耐性、原像耐性は似ているが異なる概念である。署名や証明書ではハッシュの安全性が重要になる。

Q049 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

送信者Aが文書にデジタル署名し、受信者BがAの署名を検証する。一般的な公開鍵署名方式で用いる鍵の組合せとして、最も適切なものはどれか。
ア．AがBの公開鍵で署名し、BがBの秘密鍵で検証する。
イ．AがAの秘密鍵で署名し、BがAの公開鍵で検証する。
ウ．AとBが同じ共通鍵で署名し、第三者も同じ鍵で検証する。
エ．AがAの公開鍵で署名し、BがAの秘密鍵で検証する。

正答・4肢解説・総合解説

正答：イ．AがAの秘密鍵で署名し、BがAの公開鍵で検証する。
ア：これは機密通信の暗号化に近い組合せであり、Aの署名者性を示す署名方式ではない。
イ：デジタル署名では署名者だけが秘密鍵を保持し、検証者は対応する公開鍵で署名を検証する。
ウ：共通鍵では第三者に対してどちらが生成したかを区別しにくく、通常の公開鍵デジタル署名とは異なる。
エ：秘密鍵は署名者が秘匿し、検証者へ渡すものではない。
総合解説：署名は主に完全性、署名者の認証、否認防止に寄与する。機密性を得るには別途暗号化が必要である。

Q050 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

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．秘密鍵を全利用者へ安全に配布する。
イ．全ての通信内容を自動的に圧縮する。
ウ．OSの仮想記憶領域を拡張する。
エ．公開鍵と、その所有者を示す識別情報などの対応を、認証局の署名等によって検証可能にする。

正答・4肢解説・総合解説

正答：エ．公開鍵と、その所有者を示す識別情報などの対応を、認証局の署名等によって検証可能にする。
ア：秘密鍵は所有者が秘匿すべきであり、証明書で配布するものではない。
イ：公開鍵証明書の目的は公開鍵と主体の対応を証明することであり、通信内容の圧縮ではない。
ウ：仮想記憶はOSのメモリ管理機能であり、証明書とは無関係である。
エ：証明書は公開鍵が誰に属するかを検証するための仕組みで、PKIの重要な要素である。
総合解説：証明書を信頼するには、発行したCAの信頼、証明書の有効期限、失効状態、名前の一致なども確認する必要がある。

Q051 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

公開鍵証明書が有効期限内であっても、秘密鍵漏えいなどにより途中で失効していないか確認する代表的な仕組みはどれか。
ア．CRLやOCSPを利用して失効状態を確認する。
イ．ARPでMACアドレスを確認する。
ウ．RAID 1で証明書を二重化する。
エ．DNSのTTLを0にする。

正答・4肢解説・総合解説

正答：ア．CRLやOCSPを利用して失効状態を確認する。
ア：証明書は有効期限だけでなく、CAが失効させていないか確認する必要がある。CRLとOCSPは代表的な失効確認手段である。
イ：ARPはLAN内のIP-MAC対応を解決する仕組みで、証明書失効確認には使わない。
ウ：ストレージ冗長化は証明書の信頼状態を確認する仕組みではない。
エ：DNS TTLはキャッシュ保持時間に関する値で、証明書失効を示さない。
総合解説：証明書検証では、署名チェーン、有効期間、失効、利用目的、ホスト名等を総合的に確認する。

Q052 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

大量データを安全かつ効率的に暗号化するため、共通鍵暗号と公開鍵暗号を組み合わせる代表的な理由として最も適切なものはどれか。
ア．公開鍵暗号は一切鍵を使わないため。
イ．共通鍵暗号はハッシュ値しか生成できないため。
ウ．両方式を組み合わせると証明書検証が不要になるため。
エ．データ本体は高速な共通鍵暗号で処理し、その共通鍵の配送・保護に公開鍵暗号を利用できるから。

正答・4肢解説・総合解説

正答：エ．データ本体は高速な共通鍵暗号で処理し、その共通鍵の配送・保護に公開鍵暗号を利用できるから。
ア：公開鍵暗号も公開鍵と秘密鍵の鍵ペアを使用するため、鍵を使わない方式ではない。
イ：共通鍵暗号はデータの暗号化・復号に用いる方式である。
ウ：公開鍵の真正性を確かめる必要は残り、PKI等の検証が重要である。
エ：ハイブリッド方式は、共通鍵暗号の処理性能と公開鍵暗号の鍵配送上の利便性を組み合わせる。
総合解説：TLSなど多くの実用プロトコルでは、鍵合意や認証とデータ暗号化で異なる暗号技術を組み合わせている。

Q053 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

HMACの主な用途として、最も適切なものはどれか。
ア．メッセージ内容を第三者から読めないよう暗号化する。
イ．秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成し、完全性と送信元認証を支援する。
ウ．IPアドレスをMACアドレスへ変換する。
エ．公開鍵証明書を発行する。

正答・4肢解説・総合解説

正答：イ．秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成し、完全性と送信元認証を支援する。
ア：HMACは機密性を提供する暗号化方式ではない。
イ：HMACは共有秘密とハッシュ関数を用いて、メッセージが改ざんされていないことと鍵を知る主体が生成したことを確認する。
ウ：IPアドレスとMACアドレスの対応解決はARPの機能であり、HMACの用途ではない。
エ：証明書発行はCA等のPKI機能であり、HMACの役割ではない。
総合解説：HMACはデジタル署名と異なり共通秘密を使うため、第三者に対する否認防止の性質は一般に持たない。

Q054 1-2 セキュリティ基礎 / 暗号・ハッシュ・PKI

同じパスワードを使う利用者同士でも保存ハッシュ値が同じになりにくくし、事前計算済みテーブルによる攻撃を困難にしたい。最も適切な対策はどれか。
ア．全利用者で同じ固定saltを永続的に使う。
イ．パスワードを平文のまま保存する。
ウ．利用者ごとに十分ランダムなsaltを付加してパスワードハッシュを計算する。
エ．パスワードの文字列をBase64で変換して保存する。

正答・4肢解説・総合解説

正答：ウ．利用者ごとに十分ランダムなsaltを付加してパスワードハッシュを計算する。
ア：固定共通saltでは利用者ごとの差を作れず、事前計算攻撃への効果も限定される。
イ：漏えい時に直ちに認証情報が露出するため不適切である。
ウ：saltはパスワードごとに異なる入力を作ることで、同一パスワードのハッシュ一致や事前計算攻撃を困難にする。
エ：Base64は可逆な符号化であり、パスワード保護のためのハッシュではない。
総合解説：saltは秘密である必要はないが、十分にランダムで利用者ごとに異なることが重要である。実運用では適切なパスワードハッシュ/KDFも選ぶ。

Q055 1-2 セキュリティ基礎 / 認証・アクセス制御

認証（Authentication）と認可（Authorization）の違いとして、最も適切なものはどれか。
ア．認証は権限付与、認可は本人確認だけを行う。
イ．認証と認可は完全に同じ意味である。
ウ．認可は暗号化鍵の長さを決める処理である。
エ．認証は主体が誰であるかを確かめ、認可はその主体にどの操作を許可するかを決定する。

正答・4肢解説・総合解説

正答：エ．認証は主体が誰であるかを確かめ、認可はその主体にどの操作を許可するかを決定する。
ア：認証は主体確認、認可は権限判断であり、選択肢の説明は両者を逆にしている。
イ：認証と認可は連続して使われることが多いが、本人確認と権限判断という異なる概念である。
ウ：認可は操作権限の判断であり、鍵長決定ではない。
エ：本人確認とアクセス権限の判断は別プロセスとして区別する必要がある。
総合解説：ログインに成功しても、全ての操作を許されるわけではない。認証後に認可でアクセス範囲を制御する。

Q056 1-2 セキュリティ基礎 / 認証・アクセス制御

多要素認証（MFA）の組合せとして、最も適切なものはどれか。
ア．パスワードと、利用者が所持するハードウェア認証器を組み合わせる。
イ．パスワードと秘密の質問を組み合わせる。
ウ．PINと暗証番号を組み合わせる。
エ．同じパスワードを2回入力する。

正答・4肢解説・総合解説

正答：ア．パスワードと、利用者が所持するハードウェア認証器を組み合わせる。
ア：知識要素と所持要素など、異なる種類の認証要素を組み合わせることでMFAとなる。
イ：どちらも知識要素であり、一般に異なる要素カテゴリの組合せとはいえない。
ウ：どちらも知識要素であり、要素の多様性がない。
エ：同一要素を繰り返しても多要素認証にはならない。
総合解説：MFAでは「何個入力するか」ではなく、知識・所持・生体など異なる要素を組み合わせることが重要である。

Q057 1-2 セキュリティ基礎 / 認証・アクセス制御

経理担当者が請求書閲覧だけを行う業務システムで、不要な管理者権限まで付与されていた。最小権限の原則に沿う対応として最も適切なものはどれか。
ア．念のため全従業員へ同じ管理者権限を付与する。
イ．業務遂行に必要な閲覧権限だけを付与し、不要な管理者権限を削除する。
ウ．権限レビューを行わず、退職後もアカウントを残す。
エ．アクセスログを削除して権限管理を簡素化する。

正答・4肢解説・総合解説

正答：イ．業務遂行に必要な閲覧権限だけを付与し、不要な管理者権限を削除する。
ア：侵害時の影響を拡大し、最小権限に反する。
イ：最小権限は、利用者やプロセスへ必要最小限の権限だけを与える原則である。
ウ：不要権限・不要アカウントが残り、リスクが高まる。
エ：証跡を失い、責任追跡性や監査能力を低下させる。
総合解説：最小権限は侵害時の被害限定に有効であり、付与時だけでなく異動・退職・職務変更時の見直しも必要である。

Q058 1-2 セキュリティ基礎 / 認証・アクセス制御

多数の利用者に対し、職務「営業」「経理」「システム管理者」ごとに標準権限を定義し、利用者へ職務ロールを割り当てたい。最も適したアクセス制御方式はどれか。
ア．アクセス制御を行わず、URLを知る者全員に許可する方式。
イ．全利用者へ個別に同一の管理者権限を直接付与する方式。
ウ．DNSのレコード種別に基づき業務権限を決める方式。
エ．RBAC（Role-Based Access Control）

正答・4肢解説・総合解説

正答：エ．RBAC（Role-Based Access Control）
ア：認可を実施しておらず、職務ベース管理の要件を満たさない。
イ：役割に応じた権限分離ができず、最小権限にも反しやすい。
ウ：DNSレコードは名前解決情報であり、業務ロール管理には適さない。
エ：RBACは役割（ロール）へ権限を割り当て、利用者へロールを関連付けることで権限管理を行う。
総合解説：RBACは組織の職務構造と権限を対応付けやすい。一方、動的な属性条件が多い場合はABAC等を組み合わせることもある。

Q059 1-2 セキュリティ基礎 / 認証・アクセス制御

職務分離（Segregation of Duties）の考え方として、最も適切なものはどれか。
ア．全ての重要操作を一人の管理者に集中させる。
イ．全アカウントに同じパスワードを設定する。
ウ．重要な処理を一人だけで完結できないよう役割を分け、不正や誤操作のリスクを低減する。
エ．監査ログを記録しない。

正答・4肢解説・総合解説

正答：ウ．重要な処理を一人だけで完結できないよう役割を分け、不正や誤操作のリスクを低減する。
ア：権限集中は不正・誤操作時の影響を大きくし、職務分離と逆である。
イ：全アカウントで同一パスワードを使うと認証情報漏えい時の影響が広がり、職務分離とは無関係な不適切運用である。
ウ：申請と承認、開発と本番反映などを別の主体に分けることで、単独不正や重大なミスを抑制する。
エ：証跡を失い、牽制・監査機能を低下させる。
総合解説：職務分離は予防的管理策であり、承認、二者確認、権限分離などとして実装される。

Q060 1-2 セキュリティ基礎 / 認証・アクセス制御

従業員が退職したにもかかわらず、社内クラウドのアカウントが有効なまま残っていた。最も適切な是正策はどれか。
ア．退職手続と連動してアカウントを速やかに無効化し、必要に応じて権限・トークン・セッションも失効させる。
イ．退職者のアカウントを共有アカウントとして再利用する。
ウ．退職者へ管理者権限を追加してから無期限に保持する。
エ．ログを削除してアカウントの存在を隠す。

正答・4肢解説・総合解説

正答：ア．退職手続と連動してアカウントを速やかに無効化し、必要に応じて権限・トークン・セッションも失効させる。
ア：アカウントは作成、変更、停止、削除までライフサイクル全体で管理し、雇用終了時は不要なアクセスを迅速に遮断する。
イ：本人性・責任追跡性を損なうため不適切である。
ウ：不要な高権限アカウントを残すことになり、リスクを増大させる。
エ：ログ削除は退職者アカウントを無効化する対策にならず、さらに監査証跡まで失わせる。
総合解説：IPAシラバスでも異動、担当変更、雇用・契約終了はアクセス権レビューの重要なタイミングとして扱われる。

Q061 1-2 セキュリティ基礎 / 認証・アクセス制御

複数のクラウドサービスが、共通のIdPで認証した利用者を信頼し、各サービスで再度パスワード入力せず利用させる構成に最も関係する考え方はどれか。
ア．RAID 5
イ．IDフェデレーション／SSO
ウ．ARP
エ．データベース正規化

正答・4肢解説・総合解説

正答：イ．IDフェデレーション／SSO
ア：RAIDはディスク冗長化方式で、認証連携とは無関係である。
イ：IdPが発行するアサーション等を各サービスが信頼することで、組織横断・サービス横断の認証連携やSSOを実現できる。
ウ：ARPはIP-MAC対応を解決するプロトコルで、SSOとは関係しない。
エ：正規化はDB設計手法で、認証連携の仕組みではない。
総合解説：フェデレーションでは信頼関係、アサーションの署名・有効期限・宛先、IdP侵害時の影響などを考慮する必要がある。

Q062 1-2 セキュリティ基礎 / 認証・アクセス制御

アクセス可否を「利用者の所属部署」「端末の管理状態」「アクセス時刻」「対象データの機密区分」など複数の属性条件で動的に判断したい。最も適した考え方はどれか。
ア．ABAC（Attribute-Based Access Control）
イ．RBACだけで、時刻や端末状態を一切評価しない方式。
ウ．NAT
エ．ハッシュ関数

正答・4肢解説・総合解説

正答：ア．ABAC（Attribute-Based Access Control）
ア：ABACは主体、資源、環境などの属性をポリシーで評価し、アクセス可否を決める方式である。
イ：RBACは役割中心で、設問のような多様な動的属性条件にはABACの方が直接的に適する。
ウ：NATはアドレス変換機能であり、業務データの属性認可方式ではない。
エ：ハッシュ関数はデータのダイジェスト生成に使うもので、属性ポリシー評価を行わない。
総合解説：ゼロトラスト的なアクセス判断では、利用者・端末・資源・環境のコンテキストを継続的に評価する考え方が重要になる。

Q063 1-3 リスク・マネジメント基礎 / リスクアセスメント

情報セキュリティリスクアセスメントの基本的な流れとして、最も適切なものはどれか。
ア．暗号化し、廃棄し、再利用する。
イ．採用し、教育し、退職させる。
ウ．リスクを特定し、分析し、評価する。
エ．設計し、実装し、販売する。

正答・4肢解説・総合解説

正答：ウ．リスクを特定し、分析し、評価する。
ア：これらは個別の管理活動であり、リスクアセスメントの基本プロセスではない。
イ：人事ライフサイクルであり、リスクアセスメントの流れではない。
ウ：IPAシラバスではリスクアセスメントのプロセスとして特定、分析、評価が示されている。
エ：システム開発の流れに近く、リスクアセスメントそのものではない。
総合解説：リスクアセスメントの結果を基にリスク対応を選び、管理策や対応計画へつなげる。

Q064 1-3 リスク・マネジメント基礎 / リスクアセスメント

組織がリスク評価を行う前に「どの程度のリスクを許容するか」「どの尺度で重大度を判断するか」を定める主な目的はどれか。
ア．全リスクを必ずゼロにするため。
イ．全システムへ同一のパスワードを設定するため。
ウ．評価結果にかかわらず全リスクを受容するため。
エ．一貫したリスク評価と優先順位付けを行うためのリスク基準を確立する。

正答・4肢解説・総合解説

正答：エ．一貫したリスク評価と優先順位付けを行うためのリスク基準を確立する。
ア：リスクを完全にゼロにできるとは限らず、費用・事業目的とのバランスも必要である。
イ：全システム共通パスワードの設定は認証リスクを高めるだけで、リスク評価基準の確立とは無関係である。
ウ：リスク基準は対応判断を支えるもので、全受容を目的としない。
エ：リスク基準が明確であれば、異なるリスクを共通の判断軸で比較しやすくなる。
総合解説：リスク基準は経営方針、法令・契約、事業継続要件、リスク選好などを踏まえて定める。

Q065 1-3 リスク・マネジメント基礎 / リスクアセスメント

簡易的にリスク値を「発生可能性（1〜5）×影響度（1〜5）」で算出する組織で、発生可能性4、影響度5のリスク値はいくつか。
ア．9（4＋5として計算した値）
イ．20（4×5として計算した値）
ウ．25（最大値5×5として計算した値）
エ．45（4と5を連結しただけの値）

正答・4肢解説・総合解説

正答：イ．20（4×5として計算した値）
ア：リスク値の定義は加算ではなく乗算なので9は誤りである。
イ：定義どおり発生可能性4×影響度5=20となる。
ウ：25は両方を最大値5とした場合の値で、与えられた条件とは異なる。
エ：45は数値を連結しただけで、定義された算定式による値ではない。
総合解説：定量化の式は組織ごとに異なるため、問題文で定義された評価モデルに従う。数値だけでなく、法的・社会的影響などを別途考慮する場合もある。

Q066 1-3 リスク・マネジメント基礎 / リスクアセスメント

リスク分析で「高・中・低」の尺度を用いる方法と、推定損失額や発生頻度を数値で扱う方法の関係として、最も適切なものはどれか。
ア．定性的評価ではリスクを優先順位付けできない。
イ．定量的評価では推定誤差が一切存在しない。
ウ．前者は定性的評価、後者は定量的評価の代表例であり、目的に応じて組み合わせることもできる。
エ．両者は同時に利用してはならない。

正答・4肢解説・総合解説

正答：ウ．前者は定性的評価、後者は定量的評価の代表例であり、目的に応じて組み合わせることもできる。
ア：高・中・低等の尺度でも優先順位付けは可能である。
イ：入力データや仮定に不確実性があるため、数値でも誤差や幅を考慮する必要がある。
ウ：定性的評価は比較的導入しやすく、定量的評価は数値根拠を示しやすいが推定の不確実性に注意が必要である。
エ：定性的評価と定量的評価は排他的ではなく、組織の目的やデータ品質に応じて補完的に利用できる。
総合解説：重要なのは手法名より、評価基準が明確で再現性があり、意思決定に使えることである。

Q067 1-3 リスク・マネジメント基礎 / リスクアセスメント

固有リスク（Inherent Risk）と残留リスク（Residual Risk）の関係として、最も適切なものはどれか。
ア．固有リスクと残留リスクは必ず同じ値になる。
イ．残留リスクは管理策適用前だけに存在する。
ウ．固有リスクは管理策を考慮する前のリスク、残留リスクは管理策適用後にも残るリスクとして扱う。
エ．固有リスクは金銭的リスクだけを意味する。

正答・4肢解説・総合解説

正答：ウ．固有リスクは管理策を考慮する前のリスク、残留リスクは管理策適用後にも残るリスクとして扱う。
ア：管理策が有効に機能すれば発生可能性や影響が低下し、残留リスクは固有リスクより小さくなり得る。
イ：認証は主体確認、認可は権限判断であり、選択肢の説明は両者を逆にしている。
ウ：管理策の有効性を評価するには、対策前後でリスクがどの程度変化したかを見ることが重要である。
エ：情報セキュリティリスクには業務、法的、信用等の影響も含み得る。
総合解説：残留リスクが受容可能か、追加対応が必要かを組織のリスク基準に照らして判断する。

Q068 1-3 リスク・マネジメント基礎 / リスクアセスメント

「顧客DBが重要資産で、インターネット公開WebサーバにSQLインジェクション脆弱性があり、攻撃者が悪用してDBを不正閲覧する可能性がある」という記述で、脆弱性に該当する部分はどれか。
ア．WebサーバにSQLインジェクションが成立する弱点があること。
イ．顧客DBが重要資産であること。
ウ．攻撃者が存在すること。
エ．不正閲覧による顧客情報漏えい。

正答・4肢解説・総合解説

正答：ア．WebサーバにSQLインジェクションが成立する弱点があること。
ア：脆弱性は脅威に悪用され得る弱点であり、この例では不適切な入力処理等によりSQLインジェクションが可能な点が該当する。
イ：これは保護対象となる情報資産の説明である。
ウ：攻撃者は脅威源の一例であり、システム内部の弱点である脆弱性そのものではない。
エ：これはリスクが顕在化した際の影響・結果に該当する。
総合解説：リスクシナリオは、資産、脅威源、脅威事象、脆弱性、影響を分解すると分析しやすい。

Q069 1-3 リスク・マネジメント基礎 / リスクアセスメント

STRIDEで「攻撃者が他人のアカウントになりすます」脅威に最も対応するカテゴリはどれか。
ア．Tampering
イ．Spoofing（なりすまし）
ウ．Denial of Service
エ．Elevation of Privilege

正答・4肢解説・総合解説

正答：イ．Spoofing（なりすまし）
ア：Tamperingはデータやコードの改ざんに関する脅威である。
イ：STRIDEのSはSpoofingで、利用者やシステムの身元を偽る脅威を表す。
ウ：DoSはサービス利用を妨害する脅威である。
エ：権限昇格は本来持たない高い権限を得る脅威である。
総合解説：STRIDEはSpoofing、Tampering、Repudiation、Information Disclosure、Denial of Service、Elevation of Privilegeの観点で脅威を整理する。

Q070 1-3 リスク・マネジメント基礎 / リスクアセスメント

アタックツリー分析の説明として、最も適切なものはどれか。
ア．ネットワークの最短経路だけを計算する。
イ．全てのリスクを金額だけに変換する。
ウ．攻撃者の最終目標をルートに置き、その達成に必要な下位目標や攻撃手段をAND/ORなどで分解する。
エ．暗号鍵を木構造で保管すれば自動的に安全になる。

正答・4肢解説・総合解説

正答：ウ．攻撃者の最終目標をルートに置き、その達成に必要な下位目標や攻撃手段をAND/ORなどで分解する。
ア：これはルーティングやグラフ探索の問題であり、脅威分析としてのアタックツリーではない。
イ：アタックツリーの主目的は攻撃経路の構造化である。
ウ：アタックツリーは攻撃目標を階層化し、複数の攻撃経路や必要条件を体系的に整理する手法である。
エ：アタックツリーは脅威分析の構造化手法であり、暗号鍵を木構造で保管する方式の名称ではない。
総合解説：アタックツリーは攻撃者視点で経路を洗い出し、どの管理策がどの経路を遮断するか検討するのに役立つ。

Q071 1-3 リスク・マネジメント基礎 / リスクアセスメント

リスク所有者（Risk Owner）の説明として、最も適切なものはどれか。
ア．特定のリスクについて、管理・対応に関する説明責任や意思決定を担う者又は役割。
イ．必ず外部の攻撃者を指す。
ウ．全てのリスクを一人の技術者だけが必ず所有する。
エ．リスク評価結果を閲覧できない者を指す。

正答・4肢解説・総合解説

正答：ア．特定のリスクについて、管理・対応に関する説明責任や意思決定を担う者又は役割。
ア：リスク所有者を明確にすることで、対応の優先付けや残留リスク受容などの意思決定主体が不明確になることを防げる。
イ：攻撃者は脅威源であり、リスク所有者ではない。
ウ：組織やリスクに応じて責任者は異なり、事業側が担う場合もある。
エ：むしろリスク管理に必要な情報を得て意思決定できることが重要である。
総合解説：セキュリティ部門だけでなく、事業責任者・システム所有者等とリスクの責任を明確にすることがガバナンス上重要である。

Q072 1-3 リスク・マネジメント基礎 / リスクアセスメント

二つの脆弱性A・Bがあり、Aは技術的深刻度が高いが隔離された検証環境にあり、Bは深刻度が中程度だがインターネット公開の決済システムで実際に悪用が観測されている。対応優先度の判断として最も適切なものはどれか。
ア．常に技術的深刻度の数値だけでAを最優先にする。
イ．技術的深刻度だけでなく、露出状況、悪用状況、資産重要度、事業影響などを合わせて評価する。
ウ．実際に悪用されているBは無視し、検証環境のAだけを対応する。
エ．どちらも脆弱性なので必ず同じ優先度にする。

正答・4肢解説・総合解説

正答：イ．技術的深刻度だけでなく、露出状況、悪用状況、資産重要度、事業影響などを合わせて評価する。
ア：環境や実際の脅威、資産価値を無視すると優先順位を誤る可能性がある。
イ：リスクベースの優先順位付けでは、CVSS等の技術指標だけでなく、組織固有の環境・影響・脅威情報を組み合わせる。
ウ：実悪用と事業影響を無視しており不適切である。
エ：リスクは状況により異なるため、同一優先度とは限らない。
総合解説：脆弱性管理は「重大度順にパッチ」ではなく、脅威×露出×資産×影響を統合して判断する。

Q073 1-3 リスク・マネジメント基礎 / リスクアセスメント

情報セキュリティリスクアセスメントを見直すタイミングとして、最も適切なものはどれか。
ア．最初に一度実施した後は、組織が存続する限り見直さない。
イ．インシデント発生後だけに限定して実施する。
ウ．経営戦略やシステム変更とは無関係なので、技術部門だけで任意に決める。
エ．重大なシステム変更、新たな脅威の出現、組織・法令・事業環境の変化などがあったとき。

正答・4肢解説・総合解説

正答：エ．重大なシステム変更、新たな脅威の出現、組織・法令・事業環境の変化などがあったとき。
ア：リスク状況は変化するため一度きりでは不十分である。
イ：発生前の予防的評価や変更時の評価も必要である。
ウ：事業・組織・法規制の変化もリスクへ影響する。
エ：リスクは環境変化で変わるため、定期的な見直しに加えて重要な変更時にも再評価が必要である。
総合解説：クラウド移行、M&A、新サービス公開、法改正、重大脆弱性などはリスク見直しの契機になり得る。

Q074 1-3 リスク・マネジメント基礎 / リスクアセスメント

オンプレミスの顧客情報システムをSaaSへ移行する計画がある。リスクアセスメントで最初に行うべき考え方として最も適切なものはどれか。
ア．データ、業務、責任分界、認証、外部依存、法令・契約など移行後に変化する前提を整理してリスクを再特定する。
イ．SaaSなのでリスクは自動的にゼロになると判断する。
ウ．クラウド事業者の広告だけを根拠に評価を省略する。
エ．移行後のアクセス権やデータ所在地はリスクと無関係なので確認しない。

正答・4肢解説・総合解説

正答：ア．データ、業務、責任分界、認証、外部依存、法令・契約など移行後に変化する前提を整理してリスクを再特定する。
ア：クラウド移行は脅威・脆弱性・責任範囲・依存関係を変えるため、既存評価をそのまま流用せず再評価する必要がある。
イ：外部依存、設定ミス、アカウント侵害等のリスクは残る。
ウ：客観的な契約・認証・技術仕様等を確認する必要がある。
エ：機密性、法令、契約、業務継続に影響し得る重要要素である。
総合解説：技術変更を「製品入替え」とだけ捉えず、資産・依存関係・責任分界・脅威シナリオの変化として評価することが重要である。

Q075 1-3 リスク・マネジメント基礎 / リスク対応・管理策

リスク対応のうち「リスク回避」に最も該当する例はどれか。
ア．高リスクで代替手段があるため、該当する危険なサービスの提供自体を中止する。
イ．WAFを導入して攻撃成功確率を下げる。
ウ．サイバー保険に加入して損失の一部を補償してもらう。
エ．対策せず、残るリスクを承認して受け入れる。

正答・4肢解説・総合解説

正答：ア．高リスクで代替手段があるため、該当する危険なサービスの提供自体を中止する。
ア：リスク回避は、リスクの原因となる活動を開始しない、又は中止することでリスクを避ける対応である。
イ：WAF導入は攻撃成功可能性を下げるため、主としてリスク低減に該当する。
ウ：保険や契約による損失分担は、主としてリスク共有・移転の一例に該当する。
エ：対策を追加せず残留リスクを承認して受け入れるのは、リスク保有・受容に該当する。
総合解説：リスク対応は回避、低減、共有、保有などから選ぶ。どれが正解かは事業価値とリスク基準によって変わる。

Q076 1-3 リスク・マネジメント基礎 / リスク対応・管理策

リスク低減に最も該当する対策はどれか。
ア．脆弱性修正、MFA、ネットワーク分離などを実施し、発生可能性や影響を下げる。
イ．高リスク業務そのものを廃止する。
ウ．保険契約によって損失の一部を第三者と分担する。
エ．残留リスクを承認して受け入れる。

正答・4肢解説・総合解説

正答：ア．脆弱性修正、MFA、ネットワーク分離などを実施し、発生可能性や影響を下げる。
ア：管理策を実施してリスクの発生可能性又は影響を低下させるのがリスク低減である。
イ：高リスク業務そのものを中止する対応は、活動をやめることでリスクを避けるリスク回避に該当する。
ウ：保険や契約による損失分担は、主としてリスク共有・移転の一例に該当する。
エ：対策を追加せず残留リスクを承認して受け入れるのは、リスク保有・受容に該当する。
総合解説：低減策は技術的管理策だけでなく、教育、手順、契約、物理対策なども含む。

Q077 1-3 リスク・マネジメント基礎 / リスク対応・管理策

サイバー保険や契約による責任分担が主に該当するリスク対応はどれか。
ア．リスク共有（又は一部移転）
イ．リスク回避
ウ．リスク低減
エ．脅威の消滅

正答・4肢解説・総合解説

正答：ア．リスク共有（又は一部移転）
ア：損失の一部を保険会社や契約相手と分担することで、財務的影響等を共有する。
イ：保険や契約は業務そのものを停止する対応ではないため、リスク回避には該当しない。
ウ：管理策による発生可能性や技術的影響の低減とは区別される。
エ：保険契約をしても攻撃者や脅威そのものが消えるわけではない。
総合解説：リスク共有を選んでも、セキュリティ対策や法的責任、顧客への説明責任が全て第三者へ移るわけではない。

Q078 1-3 リスク・マネジメント基礎 / リスク対応・管理策

対策費用が非常に高い一方、発生可能性と影響が小さく、組織のリスク基準内に収まる残留リスクがある。適切な対応の選択肢として最も妥当なものはどれか。
ア．必ず事業を停止しなければならない。
イ．リスクが小さければ記録や承認は一切不要である。
ウ．受容を選べば将来の見直しは不要である。
エ．権限を持つ責任者が根拠を確認した上で、リスクを保有・受容する。

正答・4肢解説・総合解説

正答：エ．権限を持つ責任者が根拠を確認した上で、リスクを保有・受容する。
ア：低いリスクまで必ず回避する必要はなく、事業価値とのバランスを判断する。
イ：受容判断も説明責任のため記録・承認が重要である。
ウ：環境変化によりリスクが増える可能性があり、定期的な見直しが必要である。
エ：全リスクに無制限の対策を行うのではなく、リスク基準と費用対効果を踏まえて受容することも正式な対応である。
総合解説：リスク受容は「放置」ではない。評価根拠、責任者、見直し条件を明確にした意思決定である。

Q079 1-3 リスク・マネジメント基礎 / リスク対応・管理策

管理策を実施した後にも残るリスクを何と呼ぶか。
ア．残留リスク
イ．固有リスク
ウ．監査証拠
エ．可用性

正答・4肢解説・総合解説

正答：ア．残留リスク
ア：管理策はリスクを下げても完全に消せるとは限らず、対策後に残るリスクを残留リスクと呼ぶ。
イ：固有リスクは一般に管理策を考慮する前のリスクを指す。
ウ：監査証拠は監査判断を裏付ける情報であり、対策後のリスク名称ではない。
エ：可用性は情報セキュリティ特性であり、リスクの残りを表す用語ではない。
総合解説：残留リスクが受容基準を超える場合は、追加管理策や対応方法の見直しが必要になる。

Q080 1-3 リスク・マネジメント基礎 / リスク対応・管理策

次のうち、主として「検知的管理策」に該当するものはどれか。
ア．MFAを必須化して不正ログインを起こりにくくする。
イ．障害発生後にバックアップからデータを復元する。
ウ．SIEMで認証ログを相関分析し、異常なアクセスを検知してアラートを出す。
エ．高リスクサービスの提供を中止する。

正答・4肢解説・総合解説

正答：ウ．SIEMで認証ログを相関分析し、異常なアクセスを検知してアラートを出す。
ア：MFAは不正ログインの成立を事前に難しくするため、主として予防的管理策に該当する。
イ：バックアップからの復元は障害発生後に状態を回復させるため、主として是正・復旧的管理策に該当する。
ウ：検知的管理策は、発生した又は発生しつつある事象を発見することを目的とする。
エ：これは管理策分類よりリスク回避の対応に該当する。
総合解説：予防・検知・是正の管理策を組み合わせることで、単一防御が破られた場合にも被害を抑えやすくなる。

Q081 1-3 リスク・マネジメント基礎 / リスク対応・管理策

古い業務システムで直ちにMFAを導入できないが、管理者アクセスを踏み台サーバ経由に限定し、接続元制限と詳細ログ監視を強化した。この考え方に最も近いものはどれか。
ア．本来の対策ができないため、リスク評価を行わない。
イ．ログ監視はリスクに影響しないので無意味である。
ウ．本来の対策を直ちに実装できない間、リスクを抑える補完的（代替的）管理策を適用する。
エ．一時的な代替策を導入したら、恒久対策の検討は不要になる。

正答・4肢解説・総合解説

正答：ウ．本来の対策を直ちに実装できない間、リスクを抑える補完的（代替的）管理策を適用する。
ア：制約があるほど残留リスクを評価し、代替策の有効性を確認する必要がある。
イ：検知能力や追跡性を高め、リスク低減に寄与し得る。
ウ：技術的制約がある場合でも、同等又は十分なリスク低減を狙う代替策を組み合わせることがある。
エ：代替策の有効性と期限を管理し、必要に応じて恒久対策へ移行する。
総合解説：補完的管理策は「例外だから何もしない」を避けるための考え方である。制約、期間、残留リスク、監視方法を記録する。

Q082 1-3 リスク・マネジメント基礎 / リスク対応・管理策

サイバー保険に加入した組織のリスク管理として、最も適切な考え方はどれか。
ア．加入すればパッチ適用やMFAは不要になる。
イ．保険は一部の財務的損失を共有できるが、技術的管理策や法令遵守、顧客対応などの責任を不要にはしない。
ウ．加入すれば法令・契約上の義務は全て保険会社へ移る。
エ．加入すれば全ての種類の損失が無条件に全額補償される。

正答・4肢解説・総合解説

正答：イ．保険は一部の財務的損失を共有できるが、技術的管理策や法令遵守、顧客対応などの責任を不要にはしない。
ア：攻撃成功の可能性を下げる技術的対策は依然必要である。
イ：保険はリスク対応の一手段であり、侵害の発生可能性や全ての事業影響を直接なくすものではない。
ウ：法的義務や説明責任が自動的に移転するわけではない。
エ：補償範囲、免責、限度額、条件は契約ごとに異なる。
総合解説：リスク共有は管理策を代替する万能策ではない。保険条件と残留リスクを理解して組み合わせる。

Q083 1-3 リスク・マネジメント基礎 / リスク対応・管理策

年間想定損失が100万円程度のリスクに対し、毎年1億円の対策費が必要で、法令上の必須要件でもない。対応判断として最も適切なものはどれか。
ア．対策費が高いほど安全なので無条件で導入する。
イ．損失額だけでなく法的・信用・人命等も確認しつつ、費用対効果と残留リスクを比較して対応を決める。
ウ．想定損失が100万円なら法令・人命・信用影響は確認不要である。
エ．費用対効果を考えること自体が情報セキュリティでは禁止されている。

正答・4肢解説・総合解説

正答：イ．損失額だけでなく法的・信用・人命等も確認しつつ、費用対効果と残留リスクを比較して対応を決める。
ア：資源配分の妥当性を欠き、他の高リスク対策を阻害する可能性がある。
イ：リスク対応は単純に「高価な対策ほど良い」ではなく、リスク低減効果、費用、事業制約、遵守事項を総合評価する。
ウ：金銭額だけでなく、法令違反、信用低下、人命影響、事業停止なども含めて評価する必要がある。
エ：IPAシラバスでも管理策の費用算定や投資対効果が求められる。
総合解説：管理策選定では、リスク低減量とコスト、実施可能性、法令・契約、組織のリスク基準を合わせて判断する。

Q084 1-3 リスク・マネジメント基礎 / リスク対応・管理策

実効性のある情報セキュリティリスク対応計画に含める内容として、最も適切なものはどれか。
ア．製品名だけを列挙し、対象リスクや責任者は記載しない。
イ．全リスクを同じ期限・同じ優先度にする。
ウ．残留リスクは計画に含めず、存在しないものとして扱う。
エ．対象リスク、選択した対応、実施する管理策、責任者、期限、優先度、残留リスクの扱いなど。

正答・4肢解説・総合解説

正答：エ．対象リスク、選択した対応、実施する管理策、責任者、期限、優先度、残留リスクの扱いなど。
ア：対策とリスクの関係や実施責任が不明確になる。
イ：リスクの重大度や事業制約に応じて優先度を付ける必要がある。
ウ：対策後の残留リスクを評価し、受容可否を判断することが重要である。
エ：対応計画は「対策する」とだけ書くのではなく、誰が何をいつまでに実施し、どのリスクをどこまで下げるか明確にする。
総合解説：対応計画はリスクアセスメントと実行をつなぐ管理文書である。進捗、効果、変更を追跡できる形にする。

Q085 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

ISMS（情報セキュリティマネジメントシステム）の説明として、最も適切なものはどれか。
ア．ファイアウォール製品そのものの名称。
イ．組織がリスクに基づいて情報セキュリティを体系的に確立・実施・維持・改善するためのマネジメントの仕組み。
ウ．暗号アルゴリズムの国際標準だけを指す。
エ．IT部門だけが利用し、経営層は関与しない仕組み。

正答・4肢解説・総合解説

正答：イ．組織がリスクに基づいて情報セキュリティを体系的に確立・実施・維持・改善するためのマネジメントの仕組み。
ア：ファイアウォールは管理策の一つであり、ISMSそのものではない。
イ：ISMSは個別製品の導入ではなく、人・プロセス・技術を含む組織的なリスク管理の仕組みである。
ウ：ISMSは組織のマネジメントシステムであり、暗号方式だけを扱うものではない。
エ：ISMSでは組織の方針・責任・資源配分など経営関与が重要である。
総合解説：ISMSはCIAをバランスよく維持・改善し、リスクを適切に管理するための継続的な仕組みとして理解する。

Q086 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

組織の情報セキュリティ方針の役割として、最も適切なものはどれか。
ア．経営の方向性や事業要件を踏まえ、情報セキュリティに関する基本的な方向性と原則を示す。
イ．全ての具体的な操作手順を1行単位で定めることだけが目的である。
ウ．外部の法令や契約要求を無視して組織独自に決める。
エ．一度策定したら環境変化があっても改定しない。

正答・4肢解説・総合解説

正答：ア．経営の方向性や事業要件を踏まえ、情報セキュリティに関する基本的な方向性と原則を示す。
ア：方針は経営者の意図を組織へ示し、下位規程や手順、目標、管理策の整合を取る基礎となる。
イ：具体手順は下位手順書等で定めるのが一般的で、方針はより上位の方向性を示す。
ウ：方針は法令・規制・契約や利害関係者の要求も踏まえる必要がある。
エ：脅威、事業、法令、技術の変化に応じてレビュー・改定する必要がある。
総合解説：方針→規程→手順のように階層化すると、経営方針と現場運用をつなぎやすい。

Q087 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

ある企業がISMSの適用範囲を定義する際、「対象組織、拠点、業務、情報システム、外部との境界」を明確にしようとしている。この対応として最も適切な評価はどれか。
ア．適切である。適用範囲の境界と適用可能性を明確にすることはISMS運用の基礎となる。
イ．不適切である。ISMSは必ず会社全体だけを対象にし、範囲を定義してはならない。
ウ．不適切である。情報システムは範囲定義に含めてはならない。
エ．適切だが、外部委託先やインタフェースは一切考慮しなくてよい。

正答・4肢解説・総合解説

正答：ア．適切である。適用範囲の境界と適用可能性を明確にすることはISMS運用の基礎となる。
ア：範囲が曖昧だと、どの資産・部門・プロセスにリスク管理や管理策を適用するか不明確になる。
イ：組織は適用範囲を定義し、その境界と適用可能性を明確にする必要がある。
ウ：情報システムや業務は範囲検討の重要要素である。
エ：外部依存やインタフェースはリスクと責任分界に影響するため考慮が必要である。
総合解説：範囲定義では、除外の妥当性と他組織・委託先との境界も説明できるようにする。

Q088 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

ISMS運用で「文書化された情報」を管理する主な理由として、最も適切なものはどれか。
ア．文書が多いほど自動的にセキュリティが高くなるため。
イ．方針・手順・記録などを必要な状態で利用・保護し、実施内容や適合性の証拠を保持するため。
ウ．全ての文書をインターネットへ公開するため。
エ．ログや記録を残さず、監査を不要にするため。

正答・4肢解説・総合解説

正答：イ．方針・手順・記録などを必要な状態で利用・保護し、実施内容や適合性の証拠を保持するため。
ア：文書量そのものではなく、必要性と実効性が重要である。
イ：マネジメントシステムでは、必要な文書・記録を管理し、最新版の利用、改ざん防止、保存、廃棄などを統制する。
ウ：機密情報を含む場合もあり、公開範囲はアクセス制御が必要である。
エ：記録はむしろ監査・評価・改善の証拠として重要である。
総合解説：文書管理は形式的な作業ではなく、現場が正しい手順を参照できることと、実施証拠を追跡できることが目的である。

Q089 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

ISMSにおける内部監査の主な目的として、最も適切なものはどれか。
ア．監査対象部門が自分の活動を無条件で合格と判定する。
イ．脆弱性を発見しても記録せず隠す。
ウ．ISMSが組織の要求事項や適用基準に適合し、効果的に実施・維持されているかを客観的に評価する。
エ．経営者のレビューを不要にする。

正答・4肢解説・総合解説

正答：ウ．ISMSが組織の要求事項や適用基準に適合し、効果的に実施・維持されているかを客観的に評価する。
ア：客観性を損ない、監査として不適切である。
イ：監査結果は適切に記録・報告し、是正につなげる必要がある。
ウ：内部監査は運用状況を独立した視点で確認し、不適合や改善機会を明らかにする。
エ：内部監査とマネジメントレビューは役割が異なり、代替関係ではない。
総合解説：内部監査では監査基準、範囲、方法、頻度、監査員の客観性などを計画し、結果を改善へつなげる。

Q090 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

経営層が、監査結果、情報セキュリティ目標の達成状況、リスクの変化、インシデント、改善機会などを定期的に確認し、資源配分や方針変更を判断している。この活動に最も近いものはどれか。
ア．DNS名前解決
イ．トランザクションロールバック
ウ．マネジメントレビュー
エ．ARPキャッシュ更新

正答・4肢解説・総合解説

正答：ウ．マネジメントレビュー
ア：DNSはネットワークサービスであり、経営レビューではない。
イ：DB処理の原子性に関する機能であり、ISMS評価ではない。
ウ：マネジメントレビューはトップマネジメントがISMSの適切性・妥当性・有効性を評価し、必要な改善や資源に関する意思決定を行う活動である。
エ：LAN内のアドレス解決に関する処理である。
総合解説：ISMSをIT部門だけの活動にしないため、経営層が結果をレビューし、優先順位や資源を決定することが重要である。

Q091 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

内部監査で「退職者アカウントの無効化漏れ」が繰り返し発生していることが判明した。是正処置として最も適切なものはどれか。
ア．今回のアカウントだけ停止し、再発原因は調べない。
イ．監査記録を削除して不適合を無かったことにする。
ウ．漏れたアカウントを停止するだけでなく、原因を分析し、人事イベントとアカウント停止の連携手順・責任・監視を改善する。
エ．退職者アカウントを全て管理者権限へ変更する。

正答・4肢解説・総合解説

正答：ウ．漏れたアカウントを停止するだけでなく、原因を分析し、人事イベントとアカウント停止の連携手順・責任・監視を改善する。
ア：応急対応だけでは同じ不適合が繰り返される可能性が高い。
イ：監査記録を削除すると証跡を損ない、原因分析や再発防止につながる改善機会も失う。
ウ：是正処置では目の前の不適合を直すだけでなく、再発しないよう原因へ対処することが重要である。
エ：リスクをさらに高める不適切な対応である。
総合解説：「修正」と「是正処置」を区別する。修正は現象の解消、是正処置は原因への対応を含む。

Q092 1-3 リスク・マネジメント基礎 / ISMS・セキュリティポリシー

ISMSの継続的改善に関する説明として、最も適切なものはどれか。
ア．一度ISMSを構築したら、その後は変更しない。
イ．改善はインシデントが発生した場合にだけ行う。
ウ．改善とは常に新しいセキュリティ製品を購入することだけを意味する。
エ．監視・測定、監査、レビュー、インシデントや環境変化などの情報を用いて、ISMSの適切性・妥当性・有効性を継続的に高める。

正答・4肢解説・総合解説

正答：エ．監視・測定、監査、レビュー、インシデントや環境変化などの情報を用いて、ISMSの適切性・妥当性・有効性を継続的に高める。
ア：脅威・技術・事業環境は変化するため継続的な改善が必要である。
イ：監査、目標評価、法改正、技術変更なども改善の契機になる。
ウ：手順、教育、組織、契約、技術など幅広い改善がある。
エ：ISMSは認証取得や初回構築で完了するものではなく、変化するリスクに合わせて改善を続けるマネジメントシステムである。
総合解説：継続的改善は「問題が起きたら直す」だけでなく、目標・監視・評価・レビューの結果を次の対策へ反映する循環として捉える。

Q093　1-4 開発・マネジメント基礎 / 要件・設計・テスト

新しい認証システムの要件のうち、非機能要件に該当するものはどれか。
ア．平常時のログイン要求の95%を2秒以内に処理する。
イ．利用者がメールアドレスとパスワードでログインできる。
ウ．管理者が利用者アカウントを無効化できる。
エ．利用者がパスワードを変更できる。

正答・4肢解説・総合解説

正答：ア．平常時のログイン要求の95%を2秒以内に処理する。
ア：応答時間や可用性、性能、信頼性、セキュリティなどは、システムが機能をどの程度の品質で実現するかを示す非機能要件である。
イ：これはシステムが提供する具体的な機能を示す機能要件である。
ウ：これは管理機能として実現すべき機能要件である。
エ：これは利用者向けの機能要件である。
総合解説：要件定義では「何ができるか」という機能要件と、「どの程度の性能・可用性・安全性で実現するか」という非機能要件を分けて整理すると、設計・受入れ基準まで追跡しやすい。

Q094　1-4 開発・マネジメント基礎 / 要件・設計・テスト

要件トレーサビリティを確保する主な目的として、最も適切なものはどれか。
ア．要件変更を一切禁止する。
イ．各要件と設計、実装、テストとの対応関係を追跡できるようにし、漏れや不要な実装を検出しやすくする。
ウ．全ての要件を一つの文書に書けば自動的に品質を保証する。
エ．テスト工程を省略して開発期間を短縮する。

正答・4肢解説・総合解説

正答：イ．各要件と設計、実装、テストとの対応関係を追跡できるようにし、漏れや不要な実装を検出しやすくする。
ア：トレーサビリティは変更禁止の仕組みではなく、変更時の影響把握にも利用する。
イ：要件から設計・実装・テストへ、またテスト結果から元の要件へ追跡できると、変更影響や検証漏れを把握しやすい。
ウ：文書を一つにまとめるだけでは対応関係や検証結果を追跡できるとは限らない。
エ：トレーサビリティはテストの代替ではなく、むしろ要件が適切に検証されたか確認する助けになる。
総合解説：セキュリティ要件も、設計上の対策やテストケースへ結び付けて追跡できることが重要である。要件変更時は関連する設計・実装・テストへの影響を確認する。

Q095 1-4 開発・マネジメント基礎 / 要件・設計・テスト

システム開発で受入れ基準を要件定義段階から明確にする利点として、最も適切なものはどれか。
ア．開発途中の変更を無条件で認めるため。
イ．単体テストを完全に不要にするため。
ウ．利用者側が受入れ時に何を満たせば合格と判断するかを客観化し、要件の曖昧さを早期に減らせる。
エ．納品後の障害対応責任を全て利用者へ移すため。

正答・4肢解説・総合解説

正答：ウ．利用者側が受入れ時に何を満たせば合格と判断するかを客観化し、要件の曖昧さを早期に減らせる。
ア：受入れ基準は変更を無条件に認めるものではない。変更は影響や承認を管理する必要がある。
イ：受入れテストと単体テストは目的と粒度が異なり、受入れ基準が単体テストを不要にするわけではない。
ウ：受入れ基準は、成果物が業務上の要求を満たしたかを判定する物差しになる。早い段階で定義すると、要件の検証可能性も高まる。
エ：受入れ基準は責任転嫁のためではなく、要求への適合を客観的に確認するために用いる。
総合解説：「測定可能・判定可能な要件」にしておくことが重要である。例えば「高速である」ではなく、条件と応答時間などを定義するとテスト可能になる。

Q096 1-4 開発・マネジメント基礎 / 要件・設計・テスト

Webシステムで、画面表示、業務ロジック、データアクセスを適切に分離して設計する主な利点はどれか。
ア．全ての脆弱性が自動的に消滅する。
イ．データベースが不要になる。
ウ．ネットワーク障害が発生しなくなる。
エ．各層の責務と変更影響を限定しやすくなり、保守性やテスト容易性を高められる。

正答・4肢解説・総合解説

正答：エ．各層の責務と変更影響を限定しやすくなり、保守性やテスト容易性を高められる。
ア：層分離は保守性等に有効だが、入力検証や認証、設定不備など別の脆弱性対策も必要である。
イ：層分離は構造化の考え方であり、データ永続化の必要性をなくすものではない。
ウ：アプリケーション設計の分離によって物理・ネットワーク障害そのものを防げるわけではない。
エ：責務を分けることで、ある層の変更が他層へ無秩序に波及するのを抑え、再利用や単体テストもしやすくなる。
総合解説：設計原則は単なる美観ではなく、変更容易性、検証容易性、障害影響の局所化に関係する。セキュリティ機能も責務と境界を明確にして設計する。

Q097 1-4 開発・マネジメント基礎 / 要件・設計・テスト

結合テスト開始後、認証方式をパスワードのみから多要素認証へ変更する要求が出た。変更管理として最も適切な対応はどれか。
ア．要件、設計、実装、既存テスト、運用手順への影響とリスクを分析し、承認された変更として計画・反映する。
イ．重要なセキュリティ変更なので、影響分析なしで直ちに本番へ反映する。
ウ．テスト中なので要件変更は必ず拒否する。
エ．プログラムだけ変更し、要件書やテスト仕様は更新しない。

正答・4肢解説・総合解説

正答：ア．要件、設計、実装、既存テスト、運用手順への影響とリスクを分析し、承認された変更として計画・反映する。
ア：後工程の変更ほど影響範囲が広がりやすいので、関連成果物とセキュリティ・運用への影響を評価してから承認・実施する。
イ：緊急性があっても、影響や検証を無視すると新たな障害や脆弱性を生むおそれがある。
ウ：変更を禁止するのではなく、必要性、効果、コスト、リスクを評価し、正式な変更管理で判断する。
エ：成果物間の不整合が生じ、将来の保守や監査で正しい仕様を追跡できなくなる。
総合解説：変更管理では「変更内容」「理由」「影響」「承認」「実施」「検証」「文書更新」を一体として扱う。セキュリティ要件変更は運用や利用者教育まで影響することがある。

Q098 1-4 開発・マネジメント基礎 / 要件・設計・テスト

結合テストの主な目的として、最も適切なものはどれか。
ア．個々の関数やクラスを独立して詳細に検証する。
イ．複数のモジュールやコンポーネントを組み合わせ、インタフェースや連携が設計どおり動作するか確認する。
ウ．利用者が業務要件を満たすか最終確認する。
エ．本番稼働後の障害件数だけを集計する。

正答・4肢解説・総合解説

正答：イ．複数のモジュールやコンポーネントを組み合わせ、インタフェースや連携が設計どおり動作するか確認する。
ア：これは主に単体テストの目的である。
イ：結合テストでは、単体で確認済みの要素を接続したときのデータ受渡し、呼出し順序、例外処理などを重点的に確認する。
ウ：これは受入れテストの代表的な目的である。
エ：これは運用評価に近く、結合テストの目的ではない。
総合解説：単体、結合、システム、受入れなどのテストは対象と目的が異なる。どの要求をどのレベルで検証するかを設計しておくことが重要である。

Q099 1-4 開発・マネジメント基礎 / 要件・設計・テスト

年齢入力が「18以上65以下」の整数だけを有効とする仕様で、境界値分析の観点から優先度が高いテストデータの組合せはどれか。
ア．20、30、40、50（範囲内の代表値だけ）
イ．1、2、3、4（下限から離れた無効値だけ）
ウ．17、18、65、66（下限・上限の直前と境界）
エ．18、30、50、65（境界値と範囲内代表値の組合せ）

正答・4肢解説・総合解説

正答：ウ．17、18、65、66（下限・上限の直前と境界）
ア：境界から離れた範囲内の値だけであり、境界値分析の優先データとしては弱い。
イ：無効値ではあるが下限18の直前・境界や上限65の境界・直後を直接確認できない。
ウ：下限18の直前17と境界18、上限65の境界65と直後66を含み、境界値分析として優先度が高い。
エ：下限・上限そのものは含むが、その直前・直後を欠くため境界の外側での判定を十分確認できない。
総合解説：「以上」「以下」「未満」などの比較演算子の誤りは境界付近で現れやすい。等価分割と組み合わせると効率的にテストケースを設計できる。

Q100 1-4 開発・マネジメント基礎 / 要件・設計・テスト

不具合修正後に回帰テスト（リグレッションテスト）を実施する主な目的はどれか。
ア．修正した箇所だけを初めてテストする。
イ．本番データを必ず削除して初期化する。
ウ．利用者教育の理解度を測定する。
エ．修正によって、以前は正常だった機能に新たな不具合が生じていないことを確認する。

正答・4肢解説・総合解説

正答：エ．修正によって、以前は正常だった機能に新たな不具合が生じていないことを確認する。
ア：修正箇所の確認だけでは、周辺機能への副作用を見落とす可能性がある。
イ：回帰テストの目的は既存機能への影響確認であり、本番データ削除は要件ではない。
ウ：これは教育評価であり、ソフトウェア変更による退行の検出とは異なる。
エ：変更は想定外の範囲へ影響することがあるため、既存機能が劣化していないか再確認する。
総合解説：修正確認（fix verification）と回帰テストは区別する。前者は原因が直ったか、後者は変更による副作用がないかを確認する。

Q101 1-4 開発・マネジメント基礎 / 要件・設計・テスト

要件書に「重要な操作は安全に記録する」とだけ書かれている。監査ログ要件として改善する際、最も適切な記述はどれか。
ア．対象操作、記録項目、時刻同期、アクセス権、保持期間、改ざん防止、監視・確認方法などを明確にする。
イ．「ログは多ければ多いほどよい」とだけ追記する。
ウ．ログは開発者だけが自由に削除できるようにする。
エ．ログ要件は運用段階で初めて考える。

正答・4肢解説・総合解説

正答：ア．対象操作、記録項目、時刻同期、アクセス権、保持期間、改ざん防止、監視・確認方法などを明確にする。
ア：「安全に」のような抽象表現を、何を、どの条件で、どの程度保護・保存・確認するかへ具体化すると設計・テスト可能になる。
イ：量だけでは目的に必要なイベントや保護要件を判断できず、過剰収集による負荷やプライバシー問題も起こり得る。
ウ：重要な証跡を容易に削除できる設計は、改ざん防止や説明責任の観点で不適切である。
エ：設計後に追加すると必要なイベント情報が取得できない可能性があるため、要件・設計段階から検討する。
総合解説：セキュリティ要件も受入れ可能な判定基準を持つ必要がある。ログでは「取得すること」だけでなく、保護・保持・監視・利用目的まで定義する。

Q102 1-4 開発・マネジメント基礎 / 要件・設計・テスト

開発者による自己テストに加えて、独立したテスト担当者による確認を行う利点として、最も適切なものはどれか。
ア．独立担当者が確認すれば、欠陥が存在しないことを数学的に証明できる。
イ．開発者自身の思い込みや確認漏れとは異なる視点で欠陥を発見できる可能性が高まる。
ウ．開発者による単体テストは不要になる。
エ．独立担当者は仕様を知らない方が常に高品質になる。

正答・4肢解説・総合解説

正答：イ．開発者自身の思い込みや確認漏れとは異なる視点で欠陥を発見できる可能性が高まる。
ア：通常のテストで欠陥がないことを完全に証明することはできない。テストは欠陥の存在を示せても不在を保証しきれない。
イ：独立性のある視点は、仕様解釈や正常系への偏りなど、作成者が気付きにくい問題の発見に役立つ。
ウ：異なるテストには役割があり、独立したテストが開発者の検証を全て置き換えるわけではない。
エ：適切なテストには対象や要求の理解が必要であり、独立性は無知であることを意味しない。
総合解説：テストの独立性は品質向上に有効だが、完全性を保証する魔法ではない。リスクに応じてレビュー、自動テスト、受入れ確認など複数の品質活動を組み合わせる。

Q103 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

WBS（Work Breakdown Structure）の主な目的はどれか。
ア．組織の財務諸表を作成する。
イ．ネットワークの経路を自動計算する。
ウ．プロジェクトの成果物や作業を管理可能な単位へ階層的に分解し、スコープや見積りの基礎にする。
エ．全てのリスクをゼロにする。

正答・4肢解説・総合解説

正答：ウ．プロジェクトの成果物や作業を管理可能な単位へ階層的に分解し、スコープや見積りの基礎にする。
ア：WBSはプロジェクト作業の分解構造であり、財務諸表作成の手法ではない。
イ：ルーティングの計算とは無関係である。
ウ：WBSは必要な作業を構造化して見える化し、担当、期間、コストなどの計画につなげるために用いる。
エ：WBSはリスク管理にも情報を与えるが、リスクをゼロにする仕組みではない。
総合解説：WBSが粗すぎると見積りや進捗把握が難しく、細かすぎると管理負荷が増える。目的に合う粒度で分解することが重要である。

Q104 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

あるプロジェクトで、開始から終了までの経路Aは12日、経路Bは15日、経路Cは10日かかる。依存関係が固定され、各経路の所要時間がそのまま完了時期を決めるとき、クリティカルパスはどれか。
ア．経路A
イ．経路C
ウ．全ての経路
エ．経路B

正答・4肢解説・総合解説

正答：エ．経路B
ア：12日は最長ではないため、この条件ではクリティカルパスではない。
イ：10日は最短であり、この条件では完了時期を制約しない。
ウ：所要時間が異なるので、全経路が同時にクリティカルになるわけではない。
エ：最長所要時間の経路B（15日）がプロジェクト完了時期を制約するため、クリティカルパスになる。
総合解説：クリティカルパス上の作業遅延は、余裕を確保しない限りプロジェクト全体の完了遅延につながる。短縮策は依存関係やリスクも含めて評価する。

Q105 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

ある時点でPV（計画価値）=100、EV（出来高）=80、AC（実コスト）=100である。CPI（コスト効率指数）として正しい値はどれか。
ア．0.8（EV÷AC＝80÷100）
イ．1.25（AC÷EV＝100÷80）
ウ．1.0（PV÷AC＝100÷100）
エ．0.2（PVとEVの差20を100で割った値）

正答・4肢解説・総合解説

正答：ア．0.8（EV÷AC＝80÷100）
ア：CPIはEV÷ACなので80÷100=0.8である。
イ：1.25はAC÷EVという逆数の計算であり、CPIではない。
ウ：1.0はPV÷ACの計算であり、CPIではない。
エ：0.2は計画価値と出来高の差を比率化した値であり、CPIの定義とは異なる。
総合解説：EVMではEV、PV、ACの関係から進捗とコストを定量的に把握する。CPI=EV/AC、SPI=EV/PVという定義を混同しない。

Q106 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

外部APIの仕様変更が予定されており、変更時期が自社リリースと重なる可能性がある。プロジェクトリスク管理として最も適切な初期対応はどれか。
ア．まだ発生していないので、リスクとして記録しない。
イ．発生確率と影響を評価してリスク登録し、担当者・監視条件・対応策や予備計画を定める。
ウ．影響を調べず、スケジュールを必ず1年延期する。
エ．担当者を決めず、全員が気付いたときだけ対応する。

正答・4肢解説・総合解説

正答：イ．発生確率と影響を評価してリスク登録し、担当者・監視条件・対応策や予備計画を定める。
ア：リスクは将来の不確実な事象であり、発生前に管理することに意味がある。
イ：不確実な事象は、認識した時点で評価・記録し、責任者と対応方針を明確にして監視することが基本である。
ウ：影響評価なしの極端な対応は、コストや機会損失を不必要に増やす可能性がある。
エ：責任が曖昧だと監視やエスカレーションが漏れやすい。
総合解説：リスク管理は「特定→分析→対応計画→監視」の循環で扱う。発生した問題（issue）と、まだ発生していないリスクを区別する。

Q107 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

ITサービス管理におけるインシデント管理と問題管理の関係として、最も適切なものはどれか。
ア．インシデント管理は原因分析だけを行い、復旧は行わない。
イ．問題管理は全ての利用者問い合わせを受け付ける窓口そのものである。
ウ．インシデント管理はサービスの早期復旧を重視し、問題管理は再発につながる根本原因の特定・管理を重視する。
エ．両者は名称が異なるだけで、目的も活動も完全に同じである。

正答・4肢解説・総合解説

正答：ウ．インシデント管理はサービスの早期復旧を重視し、問題管理は再発につながる根本原因の特定・管理を重視する。
ア：インシデント管理の主要目的の一つは通常サービスの早期回復である。
イ：問い合わせの受付・一次対応はサービスデスクの役割であり、問題管理の定義ではない。
ウ：同じ障害でも、利用者影響を早く戻す活動と、原因を分析して再発を減らす活動では目的が異なる。
エ：復旧優先と根本原因管理という焦点の違いがある。
総合解説：暫定回避策でサービスを復旧した後も、重大・反復する障害では問題管理によって原因、既知のエラー、恒久対策を管理する。

Q108 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

SLA（Service Level Agreement）の説明として、最も適切なものはどれか。
ア．ソフトウェアのソースコード利用許諾だけを定める契約である。
イ．プロジェクトの全作業を階層分解した図である。
ウ．障害原因を必ず一つに限定するための分析手法である。
エ．サービス提供者と顧客の間で、可用性や応答時間など合意したサービスレベルを明確にする。

正答・4肢解説・総合解説

正答：エ．サービス提供者と顧客の間で、可用性や応答時間など合意したサービスレベルを明確にする。
ア：それはソフトウェアライセンスに関する説明で、SLAの中心ではない。
イ：これはWBSの説明である。
ウ：SLAはサービスレベルの合意であり、原因分析手法ではない。
エ：SLAはサービス品質の期待値を測定可能な指標で明確にし、評価・改善の基準とする。
総合解説：SLAでは単に「高品質」と書くのではなく、測定方法、対象時間帯、除外条件、報告方法なども明確にする必要がある。

Q109 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

重要な業務システムへ緊急パッチを適用する必要がある。サービス管理上、最も適切な対応はどれか。
ア．緊急変更の手順に従って影響とリスクを評価し、必要な承認、バックアウト手順、実施後確認を行う。
イ．緊急なので変更記録は残さない。
ウ．テストも復旧手段も不要として即時適用する。
エ．全ての緊急変更は必ず次回の定期メンテナンスまで延期する。

正答・4肢解説・総合解説

正答：ア．緊急変更の手順に従って影響とリスクを評価し、必要な承認、バックアウト手順、実施後確認を行う。
ア：緊急時でも変更を無統制に実施せず、通常より迅速な経路で最低限必要な評価・承認・復旧準備を確保する。
イ：記録がないと後日の検証、監査、原因分析が困難になる。
ウ：緊急性が高くても、失敗時にサービス停止を拡大させるおそれがある。
エ：脆弱性の深刻度や悪用状況によっては延期の方が高リスクであり、一律延期は不適切である。
総合解説：変更管理の目的は「変更を遅らせること」ではなく、変更による価値とリスクを統制することにある。緊急変更にも専用の統制が必要である。

Q110 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

プロジェクトの重要な利用部門が、完成直前になって業務要件の認識違いを指摘した。この事態を予防する施策として最も適切なものはどれか。
ア．利用部門には完成まで一切情報を共有しない。
イ．早期から主要ステークホルダを特定し、要件確認やレビューに継続的に参加してもらう。
ウ．技術部門だけで業務要件を決定する。
エ．全ての要件変更を口頭だけで受け付ける。

正答・4肢解説・総合解説

正答：イ．早期から主要ステークホルダを特定し、要件確認やレビューに継続的に参加してもらう。
ア：完成時まで確認しなければ認識差が早期に検出できず、手戻りが大きくなる。
イ：影響力と関心の高いステークホルダを早期に巻き込み、合意と期待を継続的に確認することで認識差を減らせる。
ウ：業務要件は利用者・業務責任者のニーズを反映する必要があり、技術部門だけでは不十分である。
エ：記録と承認がない変更はスコープや責任の混乱につながる。
総合解説：ステークホルダ管理は連絡回数を増やすだけでなく、誰が何を決めるのか、どの成果物を確認するのかを明確にすることが重要である。

Q111 1-4 開発・マネジメント基礎 / プロジェクト・サービス管理

ITサービス継続管理の考え方として、最も適切なものはどれか。
ア．全システムを障害前と全く同じ状態へ1秒以内に戻すことだけを意味する。
イ．バックアップを一度取得すれば、その後の確認は不要である。
ウ．事業上必要なサービスについて、中断時の影響や復旧目標を踏まえて復旧・継続の能力を準備し、定期的に確認する。
エ．サービス継続は自然災害だけを対象にし、サイバー攻撃は対象外である。

正答・4肢解説・総合解説

正答：ウ．事業上必要なサービスについて、中断時の影響や復旧目標を踏まえて復旧・継続の能力を準備し、定期的に確認する。
ア：復旧目標は業務重要度やコストに応じて設定され、一律1秒ではない。
イ：バックアップは復元できることを検証し、環境や業務変化に合わせて継続的に管理する必要がある。
ウ：重要サービスを優先し、事業影響や復旧要求に基づいて代替手段、復旧手順、訓練などを準備する。
エ：サービス中断原因には災害、設備故障、サイバー攻撃など複数の要因があり得る。
総合解説：継続管理では「何を、どの時間内に、どの水準まで戻すか」を事業要件から定める。バックアップ、冗長化、代替拠点、訓練などを組み合わせる。

Q112 1-4 開発・マネジメント基礎 / 監査・内部統制

システム監査の説明として、最も適切なものはどれか。
ア．監査対象部門の代わりに日常業務を実行することが主目的である。
イ．全てのシステム設定を監査人が直接変更する活動である。
ウ．財務数値の計算だけを対象にし、IT統制は対象外である。
エ．情報システムに係るリスクへのコントロールを独立・客観的な立場から検証・評価し、組織目標の達成や説明責任に寄与する。

正答・4肢解説・総合解説

正答：エ．情報システムに係るリスクへのコントロールを独立・客観的な立場から検証・評価し、組織目標の達成や説明責任に寄与する。
ア：監査人が管理者の責任を代行すると独立性を損なうため、監査の主目的ではない。
イ：監査人は評価・報告を行い、原則として被監査部門の運用責任を引き受けない。
ウ：システム監査は情報システムや関連する管理・統制を対象にする。
エ：システム監査は、単なる障害調査ではなく、リスクとコントロールを評価し、保証や助言を通じて改善へつなげる活動である。
総合解説：監査は「運用を代行すること」と区別する。独立性・客観性を保ちながら、十分かつ適切な証拠に基づいて結論を形成する。

Q113 1-4 開発・マネジメント基礎 / 監査・内部統制

情報システム部の管理者Aが、自分で設計・承認したアクセス権管理プロセスを監査する担当者にも任命された。最も懸念される点はどれか。
ア．自己レビューとなり、監査の独立性・客観性が損なわれるおそれがある。
イ．アクセス権管理は監査対象にできない。
ウ．管理者は技術知識を持っているため、監査証拠を収集してはならない。
エ．監査では客観性より処理速度だけを優先すべきである。

正答・4肢解説・総合解説

正答：ア．自己レビューとなり、監査の独立性・客観性が損なわれるおそれがある。
ア：自ら責任を負った活動を自ら監査すると、判断の偏りや利益相反が生じる可能性が高く、独立性の確保が課題となる。
イ：アクセス権管理は重要な統制であり、システム監査の対象となり得る。
ウ：専門知識は有用だが、問題は知識の有無ではなく自己レビューによる独立性である。
エ：監査結果の信頼性には客観性が重要であり、速度だけを優先すべきではない。
総合解説：独立性は組織上の位置付けだけでなく、担当者が監査対象の設計・運用責任を負っていないかという実質面も確認する。

Q114 1-4 開発・マネジメント基礎 / 監査・内部統制

監査資源が限られている。リスクアプローチに基づく監査計画として、最も適切なものはどれか。
ア．全システムを毎回まったく同じ時間だけ監査する。
イ．事業影響、発生可能性、過去の問題、変更状況などを評価し、高リスク領域へ監査資源を重点配分する。
ウ．過去に問題がなかった領域は永久に監査対象から除外する。
エ．経営への影響を考慮せず、監査しやすい項目だけ選ぶ。

正答・4肢解説・総合解説

正答：イ．事業影響、発生可能性、過去の問題、変更状況などを評価し、高リスク領域へ監査資源を重点配分する。
ア：リスク差を無視するため、限られた監査資源を有効に配分できない。
イ：リスクアプローチでは、全領域を同じ深さで調べるのではなく、重要なリスクへ監査手続を重点化する。
ウ：環境・システム・脅威は変化するため、過去の実績だけで永久除外するのは不適切である。
エ：監査容易性ではなく、組織にとって重要なリスクを基準に優先度を決める。
総合解説：監査計画は固定ではなく、重大なインシデントやシステム変更などでリスクが変われば見直す。

Q115 1-4 開発・マネジメント基礎 / 監査・内部統制

アクセス権レビューの実施状況を監査する際、監査証拠として最も信頼性を高めやすい組合せはどれか。
ア．担当者の「毎月実施している」という口頭説明だけに依存する。
イ．手順書が存在することだけを確認し、実施記録は見ない。
ウ．承認記録、実際の権限一覧、システムログを突合し、必要に応じ担当者へ質問して整合性を確認する。
エ．監査人の経験だけで、証拠を収集せず結論を出す。

正答・4肢解説・総合解説

正答：ウ．承認記録、実際の権限一覧、システムログを突合し、必要に応じ担当者へ質問して整合性を確認する。
ア：口頭説明は有用だが、単独では実施実績や内容を十分に裏付けにくい。
イ：規程の存在と実際の運用は別であり、運用有効性を判断できない。
ウ：複数種類の証拠を突合すると、単なる口頭説明だけより事実を客観的に裏付けやすい。
エ：監査結論は十分かつ適切な証拠に基づく必要がある。
総合解説：証拠は量だけでなく、関連性、信頼性、十分性が重要である。文書、ログ、観察、再実施、質問などをリスクに応じて組み合わせる。

Q116 1-4 開発・マネジメント基礎 / 監査・内部統制

監査調書を作成・保管する主な目的として、最も適切なものはどれか。
ア．被監査部門の全業務を監査人が代行した証明にする。
イ．監査報告書を作成しないための代替物にする。
ウ．証拠を残さず、監査人の記憶だけで結論を再現する。
エ．実施した監査手続、入手した証拠、判断過程などを記録し、監査結論の根拠と品質管理に利用する。

正答・4肢解説・総合解説

正答：エ．実施した監査手続、入手した証拠、判断過程などを記録し、監査結論の根拠と品質管理に利用する。
ア：監査調書は業務代行の記録ではなく、監査実施と判断の記録である。
イ：監査調書は内部の作業記録であり、必要な監査報告の代替ではない。
ウ：調書はむしろ証拠と判断を記録し、後から検証できるようにするために作る。
エ：監査調書は、何をどのように確認し、どの証拠に基づきどの結論へ至ったかを追跡できるようにする。
総合解説：監査調書には機密情報が含まれる場合があるため、作成するだけでなくアクセス制御や保管・廃棄も適切に管理する。

Q117 1-4 開発・マネジメント基礎 / 監査・内部統制

経費支払システムで、一人の担当者が取引先登録、請求入力、支払承認、振込データ送信まで全て実行できる。内部統制上、最も直接的な改善策はどれか。
ア．取引登録、承認、支払実行など相反する職務を分離し、必要に応じ相互確認を行う。
イ．その担当者の権限をさらに増やす。
ウ．ログを全て無効化して処理速度を上げる。
エ．承認を口頭だけにして記録を残さない。

正答・4肢解説・総合解説

正答：ア．取引登録、承認、支払実行など相反する職務を分離し、必要に応じ相互確認を行う。
ア：一人で取引作成から支払まで完結できると、不正や誤りを隠しやすい。職務分離は相互牽制を働かせる代表的な予防統制である。
イ：権限集中を強めるため、不正や誤りのリスクを高める。
ウ：証跡が失われ、検知・追跡能力が低下する。
エ：承認の証跡がなくなり、事後検証が困難になる。
総合解説：職務分離が難しい小規模組織では、上位者レビュー、例外レポート、ログ監視などの補完統制を組み合わせる。

Q118 1-4 開発・マネジメント基礎 / 監査・内部統制

次のうち、主として発見的統制（detective control）に該当するものはどれか。
ア．最小権限に基づき、不要な管理者権限を付与しない。
イ．毎日、特権アカウントの操作ログをレビューし、異常操作を検出する。
ウ．障害で破損したデータをバックアップから復元する。
エ．入力画面で必須項目を未入力のまま登録できないようにする。

正答・4肢解説・総合解説

正答：イ．毎日、特権アカウントの操作ログをレビューし、異常操作を検出する。
ア：これは不適切な操作を事前に防ぐことを狙う予防的統制である。
イ：ログレビューは、発生した不正・異常の兆候を事後または準リアルタイムで見つけるための発見的統制である。
ウ：これは発生後の影響を修復する是正・復旧的な統制に近い。
エ：これは入力誤りを事前に防ぐ予防的統制である。
総合解説：統制は予防、発見、是正などの役割で組み合わせる。予防だけでは漏れがあり得るため、発見・復旧の仕組みも必要になる。

Q119 1-4 開発・マネジメント基礎 / 監査・内部統制

IT全般統制（ITGC）の例として、最も適切なものはどれか。
ア．売上入力時に数量×単価と明細金額の整合性を自動チェックする。
イ．請求書番号の重複登録をその業務システムで拒否する。
ウ．システム変更の申請・承認・テスト・本番反映を組織横断の手順で管理する。
エ．売上伝票の合計と総勘定元帳への転記額を照合する。

正答・4肢解説・総合解説

正答：ウ．システム変更の申請・承認・テスト・本番反映を組織横断の手順で管理する。
ア：特定業務アプリケーションの処理正確性を確保する業務処理統制の例である。
イ：特定トランザクションの入力妥当性を確保する業務処理統制である。
ウ：変更管理、アクセス管理、運用管理など、複数システムの信頼性を支える共通基盤の統制はIT全般統制に含まれる。
エ：特定業務処理の完全性・正確性を確認する統制の例であり、一般的なITGCとは異なる。
総合解説：IT全般統制が弱いと、個々のアプリケーション統制を継続的に信頼できないことがある。両者の関係を理解することが重要である。

Q120 1-4 開発・マネジメント基礎 / 監査・内部統制

監査で重大な改善提案を報告した後のフォローアップとして、最も適切なものはどれか。
ア．報告書提出後は監査人が一切関与してはならない。
イ．改善策の実施責任を監査人が全面的に引き受ける。
ウ．改善が未実施でも、記録を削除して監査を完了扱いにする。
エ．改善計画の実施状況や残存リスクを確認し、必要に応じて経営層などへ状況を報告する。

正答・4肢解説・総合解説

正答：エ．改善計画の実施状況や残存リスクを確認し、必要に応じて経営層などへ状況を報告する。
ア：基準では改善提案のフォローアップが監査活動の重要な要素として位置付けられている。
イ：改善の実施責任は通常、被監査側の管理者等にあり、監査人が代行すると独立性を損ない得る。
ウ：未解決リスクを隠す行為であり、監査の信頼性を損なう。
エ：監査報告を出して終わりにせず、合意された対応が実施され、リスクが適切に扱われているか確認する。
総合解説：フォローアップでは、期限や担当者だけでなく、対策後にリスクが許容水準まで低下したかを確認する。

Q121 1-5 企業・法務・標準 / 経営戦略・企業活動

SWOT分析で「自社が保有する高度な暗号技術の専門人材」は、一般にどの要素として整理するのが適切か。
ア．Strength（強み）
イ．Weakness（弱み）
ウ．Opportunity（機会）
エ．Threat（脅威）

正答・4肢解説・総合解説

正答：ア．Strength（強み）
ア：自社内部に存在し競争上有利に働く資源・能力はStrengthとして整理する。
イ：内部要因でも競争上不利な点を表すため、この例には該当しない。
ウ：市場拡大や法制度変更など外部環境の好機を指し、自社人材という内部資源とは異なる。
エ：競合増加や市場縮小など外部の不利な要因を指す。
総合解説：SWOTではStrength/Weaknessが内部要因、Opportunity/Threatが外部要因である。分析結果は戦略の選択肢へつなげて使う。

Q122 1-5 企業・法務・標準 / 経営戦略・企業活動

PEST分析で、個人情報保護に関する法改正は主にどの観点に分類されるか。
ア．社内の在庫回転率
イ．Political / Legalに関わる外部環境要因
ウ．特定製品のソースコード品質
エ．社員個人の目標達成率

正答・4肢解説・総合解説

正答：イ．Political / Legalに関わる外部環境要因
ア：企業内部の業務指標であり、PESTのマクロ外部環境ではない。
イ：法制度や規制の変化は、企業が直接コントロールしにくいマクロ環境として政策・法制度面で分析する。
ウ：製品内部の技術・品質要因であり、PESTで扱う社会全体の外部環境とは異なる。
エ：人事評価に関する内部指標であり、PESTの対象ではない。
総合解説：PESTは政治・法制度、経済、社会、技術などのマクロ環境を把握する枠組みである。サイバーセキュリティ経営でも規制や技術変化を外部環境として捉える。

Q123 1-5 企業・法務・標準 / 経営戦略・企業活動

「年度末までにオンライン販売の売上高を20%増加させる」をKGIとした場合、KPIの例として最も適切なものはどれか。
ア．会社の設立年月日を記録する。
イ．全社員の血液型を集計する。
ウ．月間の購入完了率やリピート購入率を継続的に測定する。
エ．KGIと同じ売上高だけを別名でKPIと呼ぶ。

正答・4肢解説・総合解説

正答：ウ．月間の購入完了率やリピート購入率を継続的に測定する。
ア：目標達成への進捗を示す指標ではない。
イ：事業目標との因果関係がなく、KPIとして不適切である。
ウ：KPIは最終目標の達成に至る途中の重要プロセスや成果を測る指標であり、売上増加へつながる行動・状態を監視する。
エ：KPIは通常、最終成果に至る重要な先行・中間指標として設定する。
総合解説：指標は測定しやすさだけで選ばず、経営目標との因果関係を考える。KGIとKPIをつなぐ仮説が重要である。

Q124 1-5 企業・法務・標準 / 経営戦略・企業活動

BPR（Business Process Reengineering）の説明として、最も適切なものはどれか。
ア．現行手順を一切変えず、処理速度だけを少し上げる。
イ．全ての業務を無条件で外部委託する。
ウ．新しいIT製品を導入すれば業務分析をしなくてもBPRになる。
エ．既存の業務プロセスを前提とせず、顧客価値や経営目標の観点から抜本的に再設計する。

正答・4肢解説・総合解説

正答：エ．既存の業務プロセスを前提とせず、顧客価値や経営目標の観点から抜本的に再設計する。
ア：これは継続的な小改善に近く、抜本的再設計を特徴とするBPRとは異なる。
イ：アウトソーシングは選択肢の一つになり得るが、BPRそのものの定義ではない。
ウ：IT導入だけでは業務プロセスの抜本的再設計とはいえない。
エ：BPRは局所的な効率化ではなく、業務の流れや役割そのものを見直して大幅な改善を狙う考え方である。
総合解説：BPRでは「現行業務をそのままIT化する」ことを避け、目的・価値・権限・プロセスを再検討する。セキュリティ統制も新しい業務に組み込む必要がある。

Q125 1-5 企業・法務・標準 / 経営戦略・企業活動

セキュリティ改善プロジェクトに500万円を投資し、年間で700万円の便益（損失回避を含む）を見込む。単純化してROIを「（便益－投資額）÷投資額」とすると、ROIは何%か。
ア．40%（指定式どおり投資額を分母にする計算）
イ．28.6%（便益を分母にする計算）
ウ．140%（便益を投資額で割るだけの計算）
エ．200%（差額200万円をそのまま200%と解釈）

正答・4肢解説・総合解説

正答：ア．40%（指定式どおり投資額を分母にする計算）
ア：指定された式では（700-500）÷500=0.4なので40%となる。
イ：28.6%は投資額ではなく便益700万円を分母にした値であり、指定式と異なる。
ウ：140%は便益700万円を投資額500万円で割った値で、投資額を差し引いていない。
エ：差額200万円という金額をそのまま200%とみなしており、率の計算になっていない。
総合解説：投資評価ではROIだけでなく、効果の不確実性、リスク低減、法令遵守、将来キャッシュフローなども考慮する。セキュリティ投資は便益の定量化が難しい場合がある。

Q126 1-5 企業・法務・標準 / 経営戦略・企業活動

固定費が600万円、製品1個の販売価格が5万円、1個当たり変動費が3万円のとき、損益分岐点販売数量はいくつか。
ア．120個（固定費600万円を販売価格5万円だけで割った値）
イ．300個（固定費600万円を1個当たり限界利益2万円で割った値）
ウ．200個（固定費600万円を1個当たり変動費3万円で割った値）
エ．600個（固定費の数値をそのまま販売数量とした値）

正答・4肢解説・総合解説

正答：イ．300個（固定費600万円を1個当たり限界利益2万円で割った値）
ア：販売価格だけで割ると変動費を考慮できず、損益分岐点数量の算定にならない。
イ：1個当たり限界利益は5万円-3万円=2万円なので、600万円÷2万円=300個である。
ウ：変動費だけで固定費を割る方法は損益分岐点数量の算定式ではない。
エ：固定費の金額の数値をそのまま数量へ置き換えることはできない。
総合解説：損益分岐点分析では、売上から変動費を差し引いた限界利益が固定費を回収する点を求める。価格や変動費の変化で損益分岐点も変わる。

Q127 1-5 企業・法務・標準 / 経営戦略・企業活動

バリューチェーン分析の主な目的として、最も適切なものはどれか。
ア．IPアドレスの経路制御表を分析する。
イ．暗号鍵の有効期限を計算する。
ウ．調達、製造、販売、サービスなどの活動がどこで価値やコストを生み、競争優位につながるかを分析する。
エ．会計仕訳だけを時系列に並べる。

正答・4肢解説・総合解説

正答：ウ．調達、製造、販売、サービスなどの活動がどこで価値やコストを生み、競争優位につながるかを分析する。
ア：これはネットワーク運用の領域であり、経営戦略のバリューチェーンとは異なる。
イ：鍵管理の技術的活動であり、バリューチェーン分析の定義ではない。
ウ：企業活動を価値創出の連鎖として捉えることで、強化すべき活動や効率化すべき活動を検討できる。
エ：財務記録の整理だけでは、価値創出活動の分析にならない。
総合解説：デジタル化によって価値連鎖が変わる場合、ITやデータが各活動をどう支えるか、また依存先のサイバーリスクがどこにあるかも併せて考えられる。

Q128 1-5 企業・法務・標準 / 経営戦略・企業活動

コアコンピタンスの説明として、最も適切なものはどれか。
ア．毎月購入する一般的な事務用品の在庫である。
イ．競合他社が公開している価格表である。
ウ．全社員が必ず同じ役職になる制度である。
エ．競合が容易に模倣しにくく、複数の事業や顧客価値の創出に生かせる企業固有の中核能力である。

正答・4肢解説・総合解説

正答：エ．競合が容易に模倣しにくく、複数の事業や顧客価値の創出に生かせる企業固有の中核能力である。
ア：一般に入手可能で競争優位の源泉となりにくい。
イ：自社固有の能力ではなく、公開された外部情報である。
ウ：中核能力の定義とは関係しない。
エ：単なる保有資産ではなく、組織に蓄積された技術・ノウハウ・能力のうち競争優位の源泉となるものを指す。
総合解説：コアコンピタンスを外部委託するか、社内に保持するかは戦略上の重要な判断である。セキュリティでも重要能力や機密ノウハウの保護が関係する。

Q129 1-5 企業・法務・標準 / 経営戦略・企業活動

顧客データを扱うシステム運用を外部委託する。経営・管理上、最も適切な考え方はどれか。
ア．業務を委託しても自社の説明責任やリスク管理が消えるわけではないため、契約・監督・評価・出口戦略を整備する。
イ．契約締結後は委託先の管理状況を一切確認しない。
ウ．委託すれば法令上の責任は全て委託先だけに移る。
エ．委託先の障害に備える必要はない。

正答・4肢解説・総合解説

正答：ア．業務を委託しても自社の説明責任やリスク管理が消えるわけではないため、契約・監督・評価・出口戦略を整備する。
ア：委託は能力やコスト面の利点がある一方、依存、情報漏えい、サービス停止などのリスクを伴う。委託先管理を継続する必要がある。
イ：委託先の環境やリスクは変化するため、継続的な監督・評価が必要である。
ウ：委託元にも法令・契約・顧客への責任が残る場合があり、一律に責任が消えるわけではない。
エ：委託依存による事業継続リスクを評価し、代替や復旧計画を検討する必要がある。
総合解説：アウトソーシングでは、選定時のデューデリジェンスだけでなく、SLA、セキュリティ要件、再委託、監査権、終了時のデータ返却・消去などを検討する。

Q130 1-5 企業・法務・標準 / 経営戦略・企業活動

既に1億円を投じたシステム開発が、将来さらに2億円必要で、完成後の便益は1億円しか見込めないと再評価された。追加投資判断で、既に支出した1億円を理由に継続を正当化する考え方の問題は何か。
ア．将来費用を必ずゼロとみなしている点。
イ．既に回収不能なサンクコストに引きずられ、将来の追加費用と便益を適切に比較できなくなる。
ウ．便益を金額で評価すること自体が禁止されている点。
エ．プロジェクトは開始したら法律上必ず完成させる必要がある点。

正答・4肢解説・総合解説

正答：イ．既に回収不能なサンクコストに引きずられ、将来の追加費用と便益を適切に比較できなくなる。
ア：問題は過去費用への固執であり、将来費用をゼロとみなすことではない。
イ：過去に支出済みで今後の意思決定によって変わらない費用は、将来の選択肢比較ではサンクコストとして区別する。
ウ：便益の定量化は意思決定に有用であり、禁止されていない。
エ：一般にそのような一律の法的義務はなく、契約や状況に応じて中止・変更を判断する。
総合解説：継続・中止判断では、将来に発生する増分コスト、期待便益、リスク、契約上の影響などを比較する。過去投資額だけで継続を決めない。

Q131 1-5 企業・法務・標準 / 経営戦略・企業活動

システム調達におけるRFP（Request for Proposal）の主な役割はどれか。
ア．受注企業が納品後に発行する請求書である。
イ．OSがCPUへ発行する割込み要求である。
ウ．発注側の要求や条件を候補ベンダへ示し、解決策、体制、費用などの提案を求める。
エ．監査人が作成する監査調書である。

正答・4肢解説・総合解説

正答：ウ．発注側の要求や条件を候補ベンダへ示し、解決策、体制、費用などの提案を求める。
ア：請求書は代金請求の文書であり、提案依頼書とは異なる。
イ：これはハードウェア・OSの割込みに関する説明で、調達文書ではない。
ウ：RFPは比較可能な提案を得るため、目的、範囲、要求、評価条件などを整理して提示する文書である。
エ：監査調書は監査手続と証拠の記録であり、提案依頼とは異なる。
総合解説：RFPにセキュリティ要件、SLA、データ取扱い、再委託条件、終了時措置などを明示すると、調達後の認識差を減らせる。

Q132 1-5 企業・法務・標準 / 経営戦略・企業活動

サービスデスクのKPIを「1件当たり対応時間の短さ」だけにしたところ、担当者が十分な確認をせず問い合わせを早く閉じる行動が増えた。改善策として最も適切なものはどれか。
ア．対応時間をさらに短くする目標だけを強化する。
イ．KPIを全て廃止し、測定を一切行わない。
ウ．問い合わせを受け付けないことで平均対応時間をゼロにする。
エ．顧客満足度、再オープン率、一次解決率なども組み合わせ、品質と効率をバランスして評価する。

正答・4肢解説・総合解説

正答：エ．顧客満足度、再オープン率、一次解決率なども組み合わせ、品質と効率をバランスして評価する。
ア：問題となっている行動をさらに促す可能性がある。
イ：測定自体をやめるのではなく、目的に合う指標設計へ改善する。
ウ：サービス目的を損ない、指標の形式的達成にすぎない。
エ：単一指標だけを強く最適化すると、本来の目的と異なる行動を誘発することがある。複数の観点で指標体系を設計する。
総合解説：指標は行動を変える。KPI設計では、測定可能性だけでなく、期待する行動と副作用を確認することが重要である。

Q133 1-5 企業・法務・標準 / 法務・コンプライアンス

個人情報保護法上の個人情報と個人データに関する説明として、最も適切なものはどれか。
ア．個人データは、個人情報データベース等を構成する個人情報として扱われ、個人情報の一部に位置付けられる。
イ．全ての個人情報は必ず個人データである。
ウ．個人データは法人に関する情報だけを意味する。
エ．個人情報は氏名だけに限られ、他の情報は含まれない。

正答・4肢解説・総合解説

正答：ア．個人データは、個人情報データベース等を構成する個人情報として扱われ、個人情報の一部に位置付けられる。
ア：個人情報と個人データは同義ではなく、個人データにはデータベース等を構成するという追加の要件がある。
イ：紙のメモなど、個人情報であっても個人情報データベース等を構成しないものは個人データに該当しない場合がある。
ウ：個人データは個人に関する情報のうち法の定義に該当するものを指す。
エ：氏名だけでなく、生存する個人を識別できる情報や個人識別符号を含むものなどが該当し得る。
総合解説：法令問題では「個人情報」「個人データ」「保有個人データ」など似た用語を区別する。義務の適用範囲が用語によって異なる。

Q134 1-5 企業・法務・標準 / 法務・コンプライアンス

顧客の個人データを扱うクラウドサービスを導入する際の対応として、最も適切なものはどれか。
ア．クラウドを使えば安全管理措置は全て事業者へ自動的に移る。
イ．取り扱うデータとリスクを把握し、必要な組織的・人的・物理的・技術的安全管理措置や委託先管理を行う。
ウ．個人データは暗号化さえすれば、アクセス権管理は不要である。
エ．漏えいが起きるまで安全管理措置を検討しない。

正答・4肢解説・総合解説

正答：イ．取り扱うデータとリスクを把握し、必要な組織的・人的・物理的・技術的安全管理措置や委託先管理を行う。
ア：利用者側に残る設定・権限・運用責任があり、法的な安全管理の検討も不要にはならない。
イ：個人データの保護は技術対策だけでなく、規程・教育・入退室・アクセス制御・委託先監督など複数の側面から行う。
ウ：暗号化だけでは不正利用や誤操作を防ぎきれず、アクセス制御等も必要である。
エ：事故前からリスクに応じた安全管理措置を講じる必要がある。
総合解説：安全管理は単一製品の導入で完了するものではない。データのライフサイクル、権限、委託・再委託、ログ、廃棄まで含めて管理する。

Q135 1-5 企業・法務・標準 / 法務・コンプライアンス

著作権に関する説明として、最も適切なものはどれか。
ア．プログラムは機械で実行されるため、著作物にはなり得ない。
イ．インターネットで公開されたプログラムは全て著作権が消滅する。
ウ．創作性のあるコンピュータプログラムは、著作権法上の著作物として保護対象になり得る。
エ．著作権はアイデアそのものを独占する権利である。

正答・4肢解説・総合解説

正答：ウ．創作性のあるコンピュータプログラムは、著作権法上の著作物として保護対象になり得る。
ア：プログラムも創作的な表現として著作物になり得る。
イ：公開しただけで著作権が当然に消滅するわけではなく、利用条件はライセンス等を確認する必要がある。
ウ：文化庁もコンピュータプログラムを著作物の例として挙げており、プログラムの著作物に関する登録制度も存在する。
エ：著作権は思想・感情の創作的な表現を保護し、アイデアそのものとは区別される。
総合解説：ソフトウェア利用では「公開されている＝自由利用」ではない。著作権とライセンス条件を区別し、複製・改変・再配布等の条件を確認する。

Q136 1-5 企業・法務・標準 / 法務・コンプライアンス

不正競争防止法上の「営業秘密」として保護を受けるための三要件の組合せはどれか。
ア．可用性・真正性・否認防止性
イ．新規性・進歩性・産業上利用可能性
ウ．機密性・完全性・可用性
エ．秘密管理性・有用性・非公知性

正答・4肢解説・総合解説

正答：エ．秘密管理性・有用性・非公知性
ア：情報セキュリティ上の性質に関する用語で、営業秘密の法定三要件ではない。
イ：主に特許要件に関する用語であり、営業秘密の要件とは異なる。
ウ：CIAは情報セキュリティの基本特性であり、不正競争防止法上の営業秘密三要件ではない。
エ：営業秘密は、秘密として管理され、事業活動に有用で、公然と知られていない情報であることが基本的な三要件である。
総合解説：営業秘密として保護したい情報は、単に「社内情報」であるだけでは足りない。秘密として管理していることを従業員等が認識できる状態にすることが重要である。

Q137 1-5 企業・法務・標準 / 法務・コンプライアンス

退職した元社員が、在職中に知った同僚のIDとパスワードを本人の承諾なく入力し、アクセス制御された社内システムへ外部からログインした。法的な論点として最も直接関係するものはどれか。
ア．不正アクセス禁止法における、他人の識別符号を無断で入力する不正アクセス行為
イ．著作権法上の引用の要件だけが問題となる。
ウ．特許出願の新規性だけが問題となる。
エ．独占禁止法の企業結合規制だけが問題となる。

正答・4肢解説・総合解説

正答：ア．不正アクセス禁止法における、他人の識別符号を無断で入力する不正アクセス行為
ア：他人のID・パスワード等の識別符号を無断で用いてアクセス制御機能を突破する行為は、不正アクセス禁止法の典型的な対象となる。
イ：この事例の中心はアクセス制御されたシステムへの無断ログインであり、引用とは直接関係しない。
ウ：無断ログインと特許の新規性は直接関係しない。
エ：企業結合ではなく、不正アクセス行為が中心論点である。
総合解説：実務では、退職者アカウントの無効化、共有パスワード禁止、多要素認証、ログ監視など技術・管理の両面で未然防止する。

Q138 1-5 企業・法務・標準 / 法務・コンプライアンス

オープンソースソフトウェアを自社製品へ組み込む際のコンプライアンス対応として、最も適切なものはどれか。
ア．無料で入手できたソフトウェアにはライセンス条件が存在しないとみなす。
イ．対象ソフトウェアのライセンス条件を確認し、著作権表示、ソース提供義務、再配布条件など該当する義務を満たす。
ウ．ライセンス文書を読まず、同じ用途の他社製品と同じ条件だと仮定する。
エ．社内で利用するだけなら、入手元やライセンスを一切記録しなくてよい。

正答・4肢解説・総合解説

正答：イ．対象ソフトウェアのライセンス条件を確認し、著作権表示、ソース提供義務、再配布条件など該当する義務を満たす。
ア：無償提供でもライセンス条件が付されることは一般的である。
イ：オープンソースは「無条件で自由」という意味ではない。各ライセンスの条件を確認して利用・配布する必要がある。
ウ：ライセンスごとに条件が異なるため、個別確認が必要である。
エ：利用形態により義務は異なるが、構成とライセンスを管理しないと将来の配布・監査時に遵守確認が困難になる。
総合解説：ソフトウェア資産管理では、名称・版・入手元・ライセンス・利用範囲を把握する。SBOM等の構成情報は脆弱性管理にも役立つ。

Q139 1-5 企業・法務・標準 / 法務・コンプライアンス

2026年1月1日から施行された、旧「下請代金支払遅延等防止法」の改正後の法律の通称として正しいものはどれか。
ア．情報流通プラットフォーム対処法
イ．個人情報保護法
ウ．中小受託取引適正化法（取適法）
エ．不正アクセス禁止法

正答・4肢解説・総合解説

正答：ウ．中小受託取引適正化法（取適法）
ア：大規模プラットフォーム上の権利侵害情報等への対応に関する別の法律であり、旧下請法の改正名称ではない。
イ：個人情報の取扱いを規律する法律であり、受託取引の適正化を目的とする法律とは異なる。
ウ：改正により法律名が「製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律」となり、略称・通称として取適法が用いられている。
エ：不正アクセス行為等を規制する法律であり、取引条件の適正化を目的としない。
総合解説：IPAの2026年版シラバスでも、法改正に対応して「下請法」を削除し「中小受託取引適正化法」を追加している。法務分野は旧称の暗記で止めず、現行名称を確認する。

Q140 1-5 企業・法務・標準 / 法務・コンプライアンス

組織のコンプライアンスを実効的に高める施策として、最も適切なものはどれか。
ア．規程を作成したら、その後の法改正を確認しない。
イ．違反を見つけても記録せず、担当者だけで隠して処理する。
ウ．教育は入社時に一度だけ行い、その後は不要とする。
エ．適用法令・契約・社内規程を特定し、責任体制、教育、相談・通報、監視、違反時の是正を継続的に運用する。

正答・4肢解説・総合解説

正答：エ．適用法令・契約・社内規程を特定し、責任体制、教育、相談・通報、監視、違反時の是正を継続的に運用する。
ア：法令や事業内容は変化するため、適用要求を継続的に見直す必要がある。
イ：再発防止や説明責任を損ない、組織的な是正ができなくなる。
ウ：役割変更、法改正、新たなリスクに応じて継続的な教育・周知が必要である。
エ：コンプライアンスは規程を置くだけでなく、適用要求の把握から教育・監視・是正まで仕組みとして運用する必要がある。
総合解説：コンプライアンスは法令だけでなく、契約、業界ルール、社内規程、倫理などを含む広い概念として扱われる。セキュリティでは違反を報告しやすい文化も重要である。

Q141 1-5 企業・法務・標準 / 法務・コンプライアンス

外部委託先へ機密情報を渡す際、NDA（秘密保持契約）を締結した。情報保護の考え方として最も適切なものはどれか。
ア．NDAだけに依存せず、必要最小限の情報提供、アクセス制御、ログ、返却・消去確認などの管理策も組み合わせる。
イ．NDAがあれば、委託先へ全情報を無制限に共有してよい。
ウ．NDAがあれば、委託終了後のデータ消去を確認する必要はない。
エ．NDAは技術的にファイルを暗号化する機能である。

正答・4肢解説・総合解説

正答：ア．NDAだけに依存せず、必要最小限の情報提供、アクセス制御、ログ、返却・消去確認などの管理策も組み合わせる。
ア：NDAは契約上の義務を明確にする重要な手段だが、不正閲覧や誤送信を技術的に防止するものではないため、他の統制が必要である。
イ：目的に不要な情報まで提供すると漏えい時の影響を拡大する。最小限の共有が重要である。
ウ：契約終了時の返却・消去はライフサイクル管理の重要事項である。
エ：NDAは契約であり、暗号化の技術機能ではない。
総合解説：契約上の統制と技術的・組織的統制を重ねる「多層防御」が実務的である。委託では再委託や事故報告、監査権も確認する。

Q142 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

JIS Q 27001:2023の位置付けとして、最も適切なものはどれか。
ア．Webアプリケーションの脆弱性だけを列挙した攻撃手法集である。
イ．ISO/IEC 27001:2022に対応した、情報セキュリティマネジメントシステム（ISMS）の要求事項を定める規格である。
ウ．暗号アルゴリズムAESの数式仕様を定める規格である。
エ．TCPの通信手順を規定するインターネット標準である。

正答・4肢解説・総合解説

正答：イ．ISO/IEC 27001:2022に対応した、情報セキュリティマネジメントシステム（ISMS）の要求事項を定める規格である。
ア：ISMSのマネジメントシステム要求事項であり、Web攻撃だけを扱う文書ではない。
イ：ISMS-ACはJIS Q 27001:2023を、ISO/IEC 27001:2022に対応したISMSの要求事項として案内している。
ウ：AESは暗号アルゴリズムの規格であり、ISMS要求事項とは異なる。
エ：TCPの仕様はRFC等で定められ、JIS Q 27001の対象ではない。
総合解説：JIS Q 27001は認証の基準となる要求事項であり、組織がリスクに基づいてISMSを構築・運用・改善する枠組みを定める。

Q143 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

Common Criteria（CC、ISO/IEC 15408）の主な目的はどれか。
ア．企業の損益分岐点を計算する。
イ．全てのネットワーク通信を自動的に暗号化する。
ウ．IT製品・システムのセキュリティ機能や保証要件を共通の基準で評価できるようにする。
エ．個人情報保護法の罰則を定める。

正答・4肢解説・総合解説

正答：ウ．IT製品・システムのセキュリティ機能や保証要件を共通の基準で評価できるようにする。
ア：会計・経営分析の手法であり、ITセキュリティ評価基準ではない。
イ：CCは評価基準であり、通信暗号化を自動実施する製品ではない。
ウ：CCはIT製品・システムのセキュリティ評価の国際的な共通基準であり、調達者、開発者、評価者が共通の枠組みで要件を扱える。
エ：法律ではなく、ITセキュリティ評価に関する標準である。
総合解説：CC認証を取得していることは、定められた評価対象・評価範囲について基準に従い評価されたことを示す。あらゆる利用環境で絶対安全という意味ではない。

Q144 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

NIST Cybersecurity Framework（CSF）2.0で、従来の5機能に加えて明示的に追加された機能はどれか。
ア．PURCHASE（購入）
イ．ENCRYPT（暗号化）
ウ．PROGRAM（プログラミング）
エ．GOVERN（統治）

正答・4肢解説・総合解説

正答：エ．GOVERN（統治）
ア：CSF 2.0の中核機能名ではない。
イ：暗号化は対策の一つだが、中核機能名ではない。
ウ：CSF 2.0の中核機能名ではない。
エ：CSF 2.0ではGOVERNが新たな中核機能として追加され、IDENTIFY、PROTECT、DETECT、RESPOND、RECOVERと合わせて6機能になった。
総合解説：GOVERNはサイバーセキュリティリスクを企業リスクや経営判断と結び付ける役割を持つ。CSF 2.0は特定業種に限定せず幅広い組織を対象としている。

Q145 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

NIST CSF 2.0を使って現状と目標のギャップを整理したい。最も適切な方法はどれか。
ア．Current Profileで現在の達成状況を表し、Target Profileで望ましい状態を定義して、差分を優先順位付けした改善計画へつなげる。
イ．全組織で同じTarget Profileを無条件に採用する。
ウ．Current Profileには将来の理想状態だけを書く。
エ．Profileを作ったらリスク変化があっても更新しない。

正答・4肢解説・総合解説

正答：ア．Current Profileで現在の達成状況を表し、Target Profileで望ましい状態を定義して、差分を優先順位付けした改善計画へつなげる。
ア：Profileは組織の状況に合わせたサイバーセキュリティ成果を表現し、現状と目標の比較に利用できる。
イ：CSFは組織の目的、リスク、資源等に合わせて活用する枠組みであり、一律の目標を強制しない。
ウ：Currentは現状を表し、将来の望ましい状態はTargetで表す。
エ：事業や脅威の変化に応じて見直し、継続的改善に利用する。
総合解説：フレームワークはチェックリストを埋めること自体が目的ではない。組織の優先順位とリスクに基づき、改善の意思決定とコミュニケーションに使う。

Q146 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」の考え方として、最も適切なものはどれか。
ア．経営者はサイバーリスクを把握せず、全責任をIT担当者へ移せばよい。
イ．サイバーセキュリティ対策を技術部門だけの課題にせず、経営者がリーダーシップを取って推進する。
ウ．サイバーセキュリティは事業継続や企業価値と無関係である。
エ．対策はインシデント発生後だけ実施すればよい。

正答・4肢解説・総合解説

正答：イ．サイバーセキュリティ対策を技術部門だけの課題にせず、経営者がリーダーシップを取って推進する。
ア：ガイドラインは経営者自身のリーダーシップと関与を重視している。
イ：同ガイドラインは経営者が認識すべき原則と、CISO等へ指示すべき重要事項を示し、経営課題としての取組を求めている。
ウ：サイバー攻撃は事業停止や信用低下につながり得るため、経営リスクとして扱う。
エ：平時からリスク管理、体制整備、訓練等を行うことが重要である。
総合解説：サイバーセキュリティは費用項目だけではなく、事業継続、競争力、信頼、法令遵守を支える経営課題として捉える。

Q147 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

自社の主要システムは堅牢だが、重要な業務を多数の委託先・クラウド事業者へ依存している。サイバーセキュリティ経営の観点で最も適切な対応はどれか。
ア．自社境界の対策が十分なら、委託先のリスクは一切考慮しない。
イ．委託先には事故が起こらないと仮定し、契約に報告義務を定めない。
ウ．自社だけでなく委託先・取引先を含むサプライチェーンのリスクを把握し、契約・評価・連携・インシデント対応を整備する。
エ．全ての委託を直ちに禁止する。

正答・4肢解説・総合解説

正答：ウ．自社だけでなく委託先・取引先を含むサプライチェーンのリスクを把握し、契約・評価・連携・インシデント対応を整備する。
ア：委託先侵害やサービス停止が自社へ波及するため、外部依存もリスク評価が必要である。
イ：事故時の連絡遅延は被害拡大につながるため、報告・連携条件を明確にする必要がある。
ウ：サプライチェーンを介した被害が拡大しており、ガイドラインでも自社のみならずサプライチェーン全体への目配りを重視している。
エ：委託には便益もあり、禁止ではなく重要度に応じてリスクを管理することが現実的である。
総合解説：サプライチェーン管理では、選定、契約、アクセス、再委託、脆弱性情報、インシデント連絡、終了時対応などライフサイクル全体で統制する。

Q148 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

IPA「情報セキュリティ10大脅威 2026」の「組織」向け脅威で1位となったものはどれか。
ア．AIの利用をめぐるサイバーリスク
イ．DDoS攻撃
ウ．内部不正による情報漏えい等
エ．ランサム攻撃による被害

正答・4肢解説・総合解説

正答：エ．ランサム攻撃による被害
ア：2026年に初選出され3位だが、1位ではない。
イ：2026年版では9位であり、1位ではない。
ウ：2026年版では7位であり、1位ではない。
エ：IPAの2026年版では「ランサム攻撃による被害」が組織向け1位で、11年連続の選出となっている。
総合解説：ランキングは社会的影響の大きかった事案等を基に選考されたもので、自組織のリスク優先順位をそのまま決めるものではない。自組織の資産・脅威・脆弱性に応じて評価する。

Q149 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

IPA「情報セキュリティ10大脅威 2026」で、組織向け脅威として初めて選出され3位となったものはどれか。
ア．AIの利用をめぐるサイバーリスク
イ．ランサム攻撃による被害
ウ．サプライチェーンや委託先を狙った攻撃
エ．ビジネスメール詐欺

正答・4肢解説・総合解説

正答：ア．AIの利用をめぐるサイバーリスク
ア：2026年版ではAI利用をめぐるサイバーリスクが初選出され、組織向け3位となった。
イ：1位であり、2026年が初選出ではない。
ウ：2位であり、以前から継続して選出されている。
エ：10位であり、以前から選出されている。
総合解説：AIの利用では、機密情報の入力、生成物の誤り、プロンプトインジェクション等の新たな論点がある。流行語として扱うのではなく、利用目的・データ・権限・外部サービス依存をリスク評価する。

Q150 1-5 企業・法務・標準 / 標準・ガイドライン・最新動向

経営会議で「IPAの10大脅威の順位どおりに予算を配分すれば、自社のリスクアセスメントは不要ではないか」という意見が出た。最も適切な回答はどれか。
ア．順位は全ての組織に法的に同じ予算配分を義務付けている。
イ．10大脅威は有用な参考情報だが、自社の資産・事業影響・脅威・脆弱性・既存対策を評価して優先順位を決める必要がある。
ウ．10大脅威に入っていない脅威は、自社では考慮してはならない。
エ．外部脅威情報はリスク管理では一切利用しない方がよい。

正答・4肢解説・総合解説

正答：イ．10大脅威は有用な参考情報だが、自社の資産・事業影響・脅威・脆弱性・既存対策を評価して優先順位を決める必要がある。
ア：10大脅威は法律による予算配分表ではない。
イ：外部の脅威情報はリスク特定に役立つが、同じ脅威でも組織ごとに曝露、影響、既存対策が異なるため、自組織の評価が必要である。
ウ：自組織固有の脅威や業界特有のリスクも存在し得る。
エ：外部情報は重要な入力情報であり、自組織の状況と組み合わせて利用する。
総合解説：標準・ガイドライン・脅威レポートは「考える枠組みや参考情報」を提供する。最終的な対策優先度は、組織の目的とリスク許容度に基づいて決める。