0001 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：基礎

TCP/IPを用いた通信に関する説明として、最も適切なものはどれか。

ア：TCPは順序制御や再送などによって信頼性のある通信を提供し、IPは宛先IPアドレスに基づいてパケットを配送する。

イ：IPが必ず到達を保証するので、TCPには再送の仕組みがない。

ウ：TCPはドメイン名をIPアドレスに変換するプロトコルである。

エ：IPは電子メールをメールボックスから取り出すためのプロトコルである。

答え・解説 正答：ア

ア：TCPとIPは役割が異なり、TCPは信頼性のある転送を、IPはネットワーク間の配送を担います。

イ：IPはベストエフォート型で、到達保証そのものを提供しません。

ウ：名前解決はDNSの役割です。

エ：メール取得はPOP3やIMAPなどの役割です。

総合解説：TCP/IPでは、ネットワーク層のIPとトランスポート層のTCPが異なる役割を分担します。障害切分けでは、どの層の機能が失敗しているかを区別することが重要です。

対象：2026年度 / 基準日 2026-09-05

0002 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：基礎

利用者がWebブラウザにホスト名を入力したときのDNSの主な役割として、最も適切なものはどれか。

ア：Webページの本文を暗号化して保存する。

イ：ホスト名などのドメイン名を、通信に用いるIPアドレスなどの情報へ対応付ける。

ウ：TCPの再送回数を決定する。

エ：電子メール本文をメールサーバ間で中継する。

答え・解説 正答：イ

ア：Webコンテンツの暗号化保存はDNSの役割ではありません。

イ：DNSはドメイン名とIPアドレスなどの情報を対応付ける分散型の名前解決システムです。

ウ：TCPの再送制御はDNSとは別の機能です。

エ：メールサーバ間の転送はSMTPの役割です。

総合解説：DNSは、人が扱いやすいドメイン名を通信に必要なアドレス情報へ結び付けます。名前解決が失敗すると、サーバ自体が稼働していてもホスト名ではアクセスできないことがあります。

対象：2026年度 / 基準日 2026-09-05

0003 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：基礎

HTTPの基本的な性質として、最も適切なものはどれか。

ア：LAN内のMACアドレスを学習してフレームを転送するプロトコルである。

イ：IPアドレスを自動配布するためだけのプロトコルである。

ウ：クライアントの要求に対してサーバが応答する、アプリケーション層のステートレスなプロトコルである。

エ：メールサーバ間でメールを中継するためのプロトコルである。

答え・解説 正答：ウ

ア：MACアドレスによるフレーム転送はL2スイッチなどの役割です。

イ：IP設定の自動配布はDHCPの役割です。

ウ：HTTPは要求・応答型で、各要求を原則として独立に扱うステートレスなアプリケーション層プロトコルです。

エ：メール転送はSMTPの役割です。

総合解説：HTTPはWebの基本となる要求・応答型プロトコルです。ステートレスであるため、継続的な利用者状態が必要なWebアプリケーションではCookieやサーバ側セッションなどを組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0004 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：標準

社内メールシステムで、メールサーバ間の配送にはSMTPを用い、利用者は複数端末から同じメールボックスを参照したい。この要件に最も適した組合せはどれか。

ア：サーバ間配送はDNS、利用者の参照にはHTTPだけを必須とする。

イ：サーバ間配送はPOP3、利用者の参照にはSMTPを用いる。

ウ：サーバ間配送も利用者の参照もDHCPで行う。

エ：サーバ間配送はSMTP、利用者によるサーバ上メールボックスの参照・同期にはIMAPを用いる。

答え・解説 正答：エ

ア：DNSは名前解決であり、メール転送そのものを担いません。

イ：SMTPとPOP3の役割が逆です。

ウ：DHCPはネットワーク設定の配布に使うプロトコルです。

エ：SMTPは転送に、IMAPはサーバ上のメールボックスを複数端末から扱う用途に適しています。

総合解説：電子メールでは、送信・中継とメールボックスへのアクセスを分けて考えます。SMTPは転送、IMAPやPOP3は利用者側の受信・参照に用いられます。

対象：2026年度 / 基準日 2026-09-05

0005 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：標準

DNSレコードの変更後、ある利用者だけがしばらく旧IPアドレスへ接続していた。原因として最も適切なものはどれか。

ア：利用者側や途中のDNSキャッシュに、TTLが満了していない旧レコードが残っている可能性がある。

イ：TCPは一度確立すると、端末再起動後も必ず旧IPアドレスを永久に記憶する。

ウ：SMTPサーバがHTTPのURLを自動的に書き換える。

エ：LANスイッチがドメイン名とIPアドレスの対応をDNSより優先して保存する。

答え・解説 正答：ア

ア：DNSでは応答を一定時間キャッシュでき、TTLが残っている間は旧情報が利用される場合があります。

イ：TCP接続はそのように永続的な名前解決情報を保持するものではありません。

ウ：SMTPはDNSキャッシュ更新を制御しません。

エ：通常のL2スイッチはDNS名前解決を代替しません。

総合解説：DNS変更の反映にはキャッシュの存在を考慮します。切替計画では事前にTTLを調整するなど、旧情報が一定期間残る可能性を踏まえます。

対象：2026年度 / 基準日 2026-09-05

0006 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：標準

1台のサーバでWebサービスとメールサービスを同時に提供できる理由の説明として、最も適切なものはどれか。

ア：DNSがサービスごとに物理NICを必ず1枚ずつ割り当てるから。

イ：IPアドレスに加えてトランスポート層のポート番号を用いることで、同じホスト上の異なる通信先サービスを区別できるから。

ウ：HTTPが全ての電子メールをWebページに変換するから。

エ：MACアドレスがアプリケーションごとに自動的に変化するから。

答え・解説 正答：イ

ア：DNSは物理NICの割当てを行いません。

イ：ポート番号により、同一IPアドレス上でも複数のアプリケーションサービスを識別できます。

ウ：HTTPは他のサービスを自動変換しません。

エ：通常、MACアドレスはネットワークインタフェースに対応し、アプリケーションごとの識別には使いません。

総合解説：IPアドレスはホストへの到達に、ポート番号はホスト上の通信エンドポイントの識別に使われます。この区別はファイアウォール設定や障害切分けの基礎にもなります。

対象：2026年度 / 基準日 2026-09-05

0007 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：標準

社内LANだけで利用するIPv4アドレスを設計する。インターネット上で一意なグローバルアドレスとして直接経路制御されることを前提にしないアドレスとして、最も適切なものはどれか。

ア：任意の他社グローバルアドレスを重複利用する。

イ：DNSサーバのIPアドレスと同じ値を全端末へ固定設定する。

ウ：RFC 1918で定められたプライベートアドレス空間を利用する。

エ：MACアドレスをそのままIPv4アドレス欄に入力する。

答え・解説 正答：ウ

ア：他組織に割り当てられたグローバルアドレスの無断利用は衝突や誤配送の原因になります。

イ：同一アドレスを複数端末へ設定するとアドレス競合が生じます。

ウ：プライベートアドレスは組織内利用を目的とし、公開インターネットでグローバルに一意な経路を前提としません。

エ：MACアドレスとIPv4アドレスは異なる識別子です。

総合解説：社内ネットワークではRFC 1918のプライベートアドレスを利用できます。インターネット接続時には、境界でのアドレス変換など別の仕組みと組み合わせることがあります。

対象：2026年度 / 基準日 2026-09-05

0008 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：応用

数百台の社内PCについて、IPアドレス、サブネットマスク、デフォルトゲートウェイなどを一元的に配布して設定作業を減らしたい。最も適切な仕組みはどれか。

ア：DNSのAレコードだけを作成すれば、各PCのIP設定も自動的に完了する。

イ：SMTPで各PCへIPアドレスをメール送信し、メール受信を設定完了条件にする。

ウ：HTTPのCookieへIPアドレスを書けばOSのネットワーク設定が自動変更される。

エ：DHCPサーバから必要なネットワーク設定を自動的に割り当てる。

答え・解説 正答：エ

ア：DNSは名前解決を行いますが、端末のIP設定配布はDHCPの役割です。

イ：SMTPはネットワーク設定配布のプロトコルではありません。

ウ：CookieはWebの状態管理に使う情報で、OSのIP設定を配布する仕組みではありません。

エ：DHCPはクライアントへIPアドレスや関連設定を動的に提供するためのプロトコルです。

総合解説：多数の端末を管理する場合、DHCPによる自動設定は運用負荷と設定ミスの低減に有効です。DNSは名前解決、DHCPは端末設定配布という役割の違いを押さえます。

対象：2026年度 / 基準日 2026-09-05

0009 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：応用

あるWebサーバへIPアドレスを直接指定すると接続できるが、通常のホスト名では接続できない。最初に確認すべき対象として最も適切なものはどれか。

ア：DNSによるホスト名の名前解決結果と、参照しているDNSサーバの状態を確認する。

イ：サーバの電源が完全に切れていると断定する。

ウ：クライアントのディスプレイ解像度を変更する。

エ：メールサーバのSMTPキューだけを削除する。

答え・解説 正答：ア

ア：IP直指定で通信できる一方、ホスト名だけ失敗する場合は、名前解決経路の確認が合理的です。

イ：IP直指定で接続できるため、サーバ停止と断定する根拠はありません。

ウ：画面解像度は名前解決障害と無関係です。

エ：Webホスト名の名前解決障害に対する第一の確認対象ではありません。

総合解説：障害切分けでは、成功している層と失敗している層を比較します。IP直指定が成功しホスト名だけ失敗するなら、DNS設定・キャッシュ・レコードを優先して確認します。

対象：2026年度 / 基準日 2026-09-05

0010 ネットワーク・システム基礎 > TCP/IP・DNS・HTTP・電子メール ｜ 難易度：標準

互いに面識のない多数の宛先へ案内メールを送る際、各受信者に他の受信者のメールアドレスを表示させたくない。最も適切な方法はどれか。

ア：全員をToに列挙し、件名に「非公開」と書く。

イ：宛先の扱いを確認した上で、他受信者から見えないBCCを利用する。

ウ：全員をCCに列挙する。

エ：DNSのTTLを0にすれば宛先アドレスが非表示になる。

答え・解説 正答：イ

ア：Toに列挙すれば各受信者にアドレスが見えるため、件名では防げません。

イ：BCCに指定した宛先は通常、他の受信者に宛先情報として表示されないため、アドレス露出を避ける用途に使われます。

ウ：CCも通常は他の受信者から宛先が見えます。

エ：DNSのTTLはメール宛先表示を制御しません。

総合解説：電子メールではTo、CC、BCCの違いを理解し、個人情報の不要な露出を避けます。ただし大量配信では誤送信防止や配信システムの利用など、組織ルールに従うことも重要です。

対象：2026年度 / 基準日 2026-09-05

0011 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：基礎

本社フロア内の端末接続と、遠隔地の支店を結ぶ拠点間接続を分類するとき、LANとWANの関係を正しく説明したものはどれか。

ア：LANは必ず無線だけで構成し、WANは必ず有線だけで構成する。

イ：LANではIPを利用できず、WANだけがTCP/IPを利用できる。

ウ：LANは建物や拠点内など比較的限定された範囲のネットワークを指し、WANは離れた拠点間など広域を接続するネットワークを指す。

エ：WANは1台のPC内部だけで完結する通信を指す。

答え・解説 正答：ウ

ア：LAN・WANの区分は有線・無線だけでは決まりません。

イ：LANでもTCP/IPは広く利用されます。

ウ：LANは比較的限定された範囲、WANは広域の拠点間接続などに用いられる分類です。

エ：WANは広域ネットワークであり、PC内部通信の意味ではありません。

総合解説：LAN/WANは主にネットワークの範囲や接続形態で区別します。セキュリティ対策を設計する際も、拠点内と拠点間で境界や通信経路が異なることを意識します。

対象：2026年度 / 基準日 2026-09-05

0012 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：基礎

L2スイッチとルータの役割の組合せとして、最も適切なものはどれか。

ア：L2スイッチはDNS名前解決だけを行い、ルータはメール保存だけを行う。

イ：L2スイッチは必ずインターネット上の経路制御を行い、ルータは同一LAN内だけを扱う。

ウ：どちらもWebページを生成するアプリケーションサーバである。

エ：L2スイッチは主にMACアドレスを基に同一LAN内のフレームを転送し、ルータはIPアドレスを基に異なるネットワーク間を中継する。

答え・解説 正答：エ

ア：どちらも説明された役割ではありません。

イ：一般的な役割が逆です。

ウ：ネットワーク機器とWebアプリケーションサーバは役割が異なります。

エ：L2スイッチとルータは参照する情報と接続範囲が異なります。

総合解説：L2スイッチは主にデータリンク層でLAN内を接続し、ルータはIPネットワーク間を接続します。障害やアクセス制御の設計では、どの機器でどの単位の通信を扱うかを区別します。

対象：2026年度 / 基準日 2026-09-05

0013 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：基礎

無線LANアクセスポイントの役割として、最も適切なものはどれか。

ア：無線LAN端末をネットワークへ接続するための無線区間の接続点となる。

イ：利用者のメール本文を長期保存するメールボックス専用装置である。

ウ：DNSのゾーン情報だけを管理する装置である。

エ：データベースのSQLを自動的に最適化する装置である。

答え・解説 正答：ア

ア：アクセスポイントはWi-Fi端末をLANへ接続するための接続点として機能します。

イ：アクセスポイントの主目的はメール保存ではありません。

ウ：DNSサーバとは別の役割です。

エ：SQL最適化は無線アクセスポイントの役割ではありません。

総合解説：無線LANではアクセスポイントを介して端末をネットワークへ収容します。SSID、認証、暗号化設定などを含め、無線区間特有の管理が必要です。

対象：2026年度 / 基準日 2026-09-05

0014 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：標準

インターネットを経由して在宅勤務者のPCと社内ネットワークを論理的に接続し、通信経路を保護したい。最も適切な技術はどれか。

ア：SSID名を社名に変更するだけで、インターネット区間の通信を保護する。

イ：VPNを利用し、共有ネットワーク上に保護された論理的な通信経路を構成する。

ウ：L2スイッチを自宅と会社に置くだけで、インターネット越しに同一LANになる。

エ：DNSキャッシュを削除することで通信内容を暗号化する。

答え・解説 正答：イ

ア：SSID名の変更だけではインターネット経路の通信保護になりません。

イ：VPNは公衆網などを利用しながら、組織内ネットワークのような論理的接続を構成するために使われます。

ウ：L2スイッチだけでは広域の安全な接続を構成できません。

エ：DNSキャッシュ削除は通信暗号化の手段ではありません。

総合解説：VPNは、インターネットなどの共有網上に保護された論理通信路を作る用途で利用されます。ただしVPNを使っても端末自体のマルウェア対策や認証管理は別途必要です。

対象：2026年度 / 基準日 2026-09-05

0015 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：標準

無線LANのSSIDに関する説明として、最も適切なものはどれか。

ア：SSIDは無線LAN暗号鍵そのものであり、公開されることはない。

イ：SSIDは端末のMACアドレスと常に同じ値でなければならない。

ウ：無線LANを識別するための名称であり、SSIDそのものを知っていることは利用者認証の代わりにはならない。

エ：SSIDを隠せば、他のセキュリティ対策は不要になる。

答え・解説 正答：ウ

ア：SSIDと暗号鍵は別の情報です。

イ：SSIDはネットワーク名であり、端末MACアドレスと一致させる必要はありません。

ウ：SSIDはネットワーク識別子であって、パスワードや利用者認証そのものではありません。

エ：SSID非表示だけで十分なセキュリティにはなりません。

総合解説：SSIDは無線LANを識別する名称です。接続制御には、適切な認証方式や暗号化、端末管理などを組み合わせる必要があります。

対象：2026年度 / 基準日 2026-09-05

0016 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：標準

PCが自分と異なるIPネットワーク上のサーバへ通信するとき、一般に最初の中継先として設定するものはどれか。

ア：WebブラウザのCookie保存先。

イ：メールソフトの署名欄。

ウ：データベースの主キー。

エ：同一LAN上のルータなどに設定されたデフォルトゲートウェイ。

答え・解説 正答：エ

ア：Cookie保存先はIP経路制御とは無関係です。

イ：電子メール署名欄はネットワーク経路とは無関係です。

ウ：主キーはDB内の行識別に使い、IP経路制御には使いません。

エ：宛先が自ネットワーク外の場合、端末は通常デフォルトゲートウェイへパケットを渡します。

総合解説：異なるIPネットワーク間の通信ではルータが経路を中継します。端末側では、自ネットワーク外宛ての既定経路としてデフォルトゲートウェイを設定するのが一般的です。

対象：2026年度 / 基準日 2026-09-05

0017 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：標準

インターネット利用者からのWeb要求をいったん受け取り、内部の複数Webサーバへ中継する構成で用いる機能として、最も適切なものはどれか。

ア：リバースプロキシ。

イ：DHCPリレーだけ。

ウ：DNSキャッシュだけ。

エ：メールクライアント。

答え・解説 正答：ア

ア：リバースプロキシは外部クライアントからの要求を受け、背後のサーバへ中継する構成で利用されます。

イ：DHCPリレーはDHCPメッセージ中継のための機能であり、Web要求中継を目的としません。

ウ：DNSキャッシュは名前解決結果の保持であり、HTTP要求の中継そのものではありません。

エ：メールクライアントはWebサーバ群へのHTTP中継装置ではありません。

総合解説：リバースプロキシはWebサーバの前段に置かれ、要求の中継、負荷分散、公開サーバの隠蔽などに利用されます。役割を通常のクライアント側プロキシと混同しないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0018 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：応用

同じフロアのPC同士は通信できるが、別拠点のサーバだけに全PCから到達できない。障害切分けの優先度が高い対象はどれか。

ア：全PCのキーボード配列。

イ：拠点間を接続するルータやWAN回線、経路設定の状態。

ウ：全PCのWebブラウザのホームページ設定だけ。

エ：各PCのローカル文書のファイル名。

答え・解説 正答：イ

ア：キーボード配列は拠点間通信の障害原因になりません。

イ：同一LAN内は正常で別拠点だけ失敗しているため、LAN-WAN境界や広域経路を優先して確認するのが合理的です。

ウ：複数PCから別拠点全般に到達できないなら、個々のブラウザ設定よりネットワーク経路を優先します。

エ：ローカルファイル名はWAN到達性と無関係です。

総合解説：障害切分けでは共通して失敗する範囲を特定します。LAN内通信が正常で別拠点への通信だけ失敗する場合、ルータ、WAN回線、ルーティングなどの共通経路を優先して確認します。

対象：2026年度 / 基準日 2026-09-05

0019 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：応用

リモート端末がVPNで社内へ安全に接続できるようにした。追加対策として最も適切な考え方はどれか。

ア：VPNを導入すれば、端末OSの更新は不要になる。

イ：VPNを導入すれば、利用者認証を廃止してよい。

ウ：VPNは通信経路の保護に有効だが、端末の認証、更新、マルウェア対策などは別途実施する。

エ：VPNを導入すれば、紛失端末からの接続リスクは自動的にゼロになる。

答え・解説 正答：ウ

ア：VPNはOS脆弱性を修正しません。

イ：VPN接続でも適切な利用者・端末認証が必要です。

ウ：VPNだけでは端末侵害や弱い認証などのリスクを解消できないため、多層的な管理が必要です。

エ：端末紛失時の資格情報悪用などは別途対策が必要です。

総合解説：VPNは重要な経路保護手段ですが、端末やアカウントの安全性まで自動的に保証するものではありません。認証、端末管理、パッチ適用、ログ監視などと組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0020 ネットワーク・システム基礎 > LAN・WAN・無線・VPN・ネットワーク機器 ｜ 難易度：標準

無線LANを新設する際の管理上の考慮として、最も適切なものはどれか。

ア：電波は必ず建物の壁で完全に止まるため、認証は不要である。

イ：SSIDを設定しなければ、端末は自動的に最強の暗号方式で接続する。

ウ：無線LANではIPアドレスやTCP/IPを利用できない。

エ：電波が物理的な配線外にも届く可能性を考え、認証・暗号化・アクセスポイント設定を適切に管理する。

答え・解説 正答：エ

ア：電波は壁の外へ届く場合があり、認証を省略すべきではありません。

イ：SSIDの有無だけで安全な認証・暗号方式が自動保証されるわけではありません。

ウ：無線LANでもTCP/IPは一般に利用されます。

エ：無線LANは電波を利用するため、物理配線だけで境界を限定できず、無線固有のアクセス管理が必要です。

総合解説：無線LANでは物理的なケーブル接続が不要なため、電波到達範囲と認証・暗号化設定を意識した管理が重要です。有線と同様のIP通信基盤を使いつつ、無線固有のリスクを加味します。

対象：2026年度 / 基準日 2026-09-05

0021 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：基礎

クライアントサーバシステムの説明として、最も適切なものはどれか。

ア：利用者側のクライアントが要求を送り、サーバが共有機能やデータなどのサービスを提供する。

イ：全端末が必ず同一処理を同時実行し、役割分担を一切しない方式である。

ウ：ネットワークを使わず1台のPC内部だけで完結する方式だけを指す。

エ：サーバは利用者の要求を受け取らず、常に一方向にデータを送るだけである。

答え・解説 正答：ア

ア：クライアントとサーバで役割を分担し、サーバが共通サービスを提供する構成です。

イ：クライアントサーバ方式は役割分担を行います。

ウ：クライアントサーバ方式は一般にネットワーク越しのサービス提供を含みます。

エ：サーバはクライアントからの要求に応じて処理する構成が一般的です。

総合解説：クライアントサーバ方式では、クライアントが利用者インタフェースや要求送信を担い、サーバが共有資源や処理を提供します。WebシステムやDBシステムの基本構成として理解します。

対象：2026年度 / 基準日 2026-09-05

0022 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：基礎

サーバ仮想化におけるVMの説明として、最も適切なものはどれか。

ア：DNSレコードの別名を表す用語である。

イ：物理サーバ上で、独立したコンピュータのように動作する仮想的な実行環境である。

ウ：電子メールの添付ファイル形式だけを表す用語である。

エ：無線LANのSSIDを暗号化する方式である。

答え・解説 正答：イ

ア：VMはDNSレコードではありません。

イ：VMは物理資源を仮想化して構成される論理的なコンピュータ環境です。

ウ：VMはメール形式ではありません。

エ：VMは無線暗号方式ではありません。

総合解説：仮想化により1台の物理サーバ上で複数のVMを動かすことができます。資源集約の利点がある一方、物理ホスト障害の影響や仮想基盤の管理も考慮します。

対象：2026年度 / 基準日 2026-09-05

0023 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：基礎

RAIDを導入したストレージに関する説明として、最も適切なものはどれか。

ア：RAIDを使えば、どの方式でも全ディスク故障時に必ずデータが残る。

イ：RAIDはネットワーク上の名前解決を高速化する技術である。

ウ：ディスク障害への耐性向上に役立つ構成があるが、誤削除やランサムウェアに備えるバックアップを完全に代替するものではない。

エ：RAIDを使うと利用者認証が不要になる。

答え・解説 正答：ウ

ア：RAIDにも耐えられる故障数の限界があります。

イ：RAIDはストレージ構成の技術で、DNSとは無関係です。

ウ：RAIDの冗長性とバックアップは目的が異なり、RAIDだけでは論理的な消失や同時破壊に十分対応できません。

エ：ストレージ冗長化と認証は別の対策です。

総合解説：RAIDはディスク冗長化や性能向上に用いられますが、バックアップとは別物です。可用性対策とデータ復旧対策を目的別に組み合わせることが重要です。

対象：2026年度 / 基準日 2026-09-05

0024 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：標準

共有ファイル置場とサーバ向け大容量ストレージを検討している。NASとSANの代表的な提供形態を正しく説明したものはどれか。

ア：NASは無線LAN専用で、SANは電子メール専用である。

イ：NASはDNSサーバの別名で、SANはDHCPサーバの別名である。

ウ：NASとSANは常に同じプロトコルと同じ接続方式でなければならない。

エ：NASはネットワーク越しにファイル共有として利用する構成が代表的で、SANはサーバへブロックレベルのストレージを提供する構成が代表的である。

答え・解説 正答：エ

ア：どちらもそのような用途限定ではありません。

イ：NAS/SANはストレージ構成の用語です。

ウ：実装や接続方式は異なり得ます。

エ：NASはファイル共有、SANはブロックストレージという利用形態で区別されるのが基本です。

総合解説：NASとSANはいずれもネットワークを利用するストレージ構成ですが、提供する単位が異なります。要件に応じてファイル共有かブロックストレージかを選択します。

対象：2026年度 / 基準日 2026-09-05

0025 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：標準

Webサービスへのアクセス増加に備えて複数サーバを並べ、要求を振り分ける。主な目的として最も適切なものはどれか。

ア：負荷を複数サーバへ分散し、性能や可用性の向上を図る。

イ：全サーバの障害を必ず同時発生させる。

ウ：DNSを使わずにドメイン名を廃止する。

エ：バックアップを取得せずにデータ消失へ備える。

答え・解説 正答：ア

ア：負荷分散は要求を複数処理系へ振り分け、過負荷軽減や冗長性向上に利用されます。

イ：負荷分散は障害を発生させるための仕組みではありません。

ウ：負荷分散とDNS利用の有無は別の論点です。

エ：負荷分散はバックアップの代替ではありません。

総合解説：負荷分散は処理能力の拡張だけでなく、一部サーバ障害時の継続運転にも利用できます。ただし共有DBなど別の単一障害点が残れば、システム全体の可用性はそこに制約されます。

対象：2026年度 / 基準日 2026-09-05

0026 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：標準

障害発生時の復旧時間をできるだけ短くしたい。通常時から待機系を稼働可能な状態にしておき、迅速に切り替える方式として最も適切なものはどれか。

ア：コールドスタンバイ。

イ：ホットスタンバイ。

ウ：フルバックアップ。

エ：DNSキャッシュ。

答え・解説 正答：イ

ア：コールドスタンバイは必要時に起動・準備するため、一般に切替え時間が長くなります。

イ：ホットスタンバイは待機系を稼働可能な状態に保ち、比較的迅速な切替えを目指す方式です。

ウ：バックアップ方式であり、待機系の稼働状態を表す方式ではありません。

エ：名前解決結果の保持であり、待機系切替方式ではありません。

総合解説：待機系の準備度合いはRTOやコストに影響します。ホットスタンバイは復旧を速めやすい一方、運用コストや同期管理が必要になります。

対象：2026年度 / 基準日 2026-09-05

0027 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：標準

あるシステムのMTBFが990時間、MTTRが10時間である。MTBF／(MTBF＋MTTR)で稼働率を求めるとき、最も適切な値はどれか。

ア：約1.0%。MTTRだけをMTBFで割る。

イ：50.0%。MTBFとMTTRを単純に平均する。

ウ：99.0%。990÷(990＋10)=0.99である。

エ：100.0%。MTBFがMTTRより長ければ常に100%になる。

答え・解説 正答：ウ

ア：10/990は故障修復時間の比に近く、指定式による稼働率ではありません。

イ：平均値を取る計算ではありません。

ウ：稼働率は990/1000=0.99、すなわち99.0%です。

エ：修復時間が存在するため100%にはなりません。

総合解説：稼働率は、平均故障間隔が長く平均修復時間が短いほど高くなります。可用性改善では故障を減らすことと、故障後の復旧を早めることの双方が有効です。

対象：2026年度 / 基準日 2026-09-05

0028 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：応用

短時間の停電でもサーバが即時停止し、データ破損が起きることを防ぎたい。最も適切な対策はどれか。

ア：DNSレコードを二重化すればサーバへ電力が供給される。

イ：RAIDだけを構成すれば停電中もサーバへ電力が供給される。

ウ：VPNを張れば停電したサーバを物理的に起動し続けられる。

エ：UPSを導入し、停電時に一時的な給電を行って継続運転や安全なシャットダウンにつなげる。

答え・解説 正答：エ

ア：DNS冗長化は電源供給の代替になりません。

イ：RAIDはストレージ冗長化であり電源装置ではありません。

ウ：VPNは通信経路を構成する技術で、電力供給はしません。

エ：UPSは電源断に対して一定時間電力を供給し、停止回避や安全な終了を支援します。

総合解説：UPSは停電や瞬断に対する電源対策ですが、長時間停電に無制限に耐えるものではありません。必要に応じて発電機、別拠点、停止手順などと組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0029 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：応用

Webサーバを2台に冗長化したが、両方が1台の共有ストレージだけに依存している。可用性評価として最も適切なものはどれか。

ア：共有ストレージが単一障害点になり得るため、サーバ冗長化だけではシステム全体の高可用性を保証できない。

イ：Webサーバが2台あれば、他の構成要素は全て単一でも停止しない。

ウ：共有ストレージが1台であるほど、必ず可用性は高くなる。

エ：サーバ台数を増やすとバックアップは不要になる。

答え・解説 正答：ア

ア：複数サーバが同じ単一資源へ依存すると、その資源障害で全体が停止する可能性があります。

イ：他の単一障害点を無視できません。

ウ：冗長性がない共有資源は障害点になり得ます。

エ：冗長化はバックアップを代替しません。

総合解説：可用性はシステム全体の依存関係で評価します。サーバ、ネットワーク、ストレージ、電源などの単一障害点を洗い出し、必要な冗長化や復旧策を設計します。

対象：2026年度 / 基準日 2026-09-05

0030 ネットワーク・システム基礎 > サーバ・ストレージ・仮想化・可用性 ｜ 難易度：標準

1台の物理ホスト上に多数のVMを集約する構成について、最も適切な説明はどれか。

ア：VMを使えば物理ホストは存在しないため、ハードウェア障害を考える必要がない。

イ：資源利用効率を高められる一方、物理ホスト障害が複数VMへ同時に影響する可能性があるため、冗長化や移行設計が重要になる。

ウ：VM同士は必ず完全に同じOSと設定でなければならない。

エ：VMを増やすほど、CPUやメモリの物理的上限は自動的に無限になる。

答え・解説 正答：イ

ア：VMも物理ハードウェア上で動作するため、基盤障害を考慮します。

イ：仮想化は集約効果がある一方、基盤障害の影響範囲が広がる可能性があります。

ウ：VMごとに異なるOSや設定を持てる場合があります。

エ：物理資源の上限は存在し、過剰割当ては性能問題の原因になります。

総合解説：仮想化は柔軟な資源配分や統合を可能にしますが、基盤の可用性や容量管理が重要です。メリットと集中リスクの双方を評価します。

対象：2026年度 / 基準日 2026-09-05

0031 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：基礎

関係データベースの表に関する説明として、最も適切なものはどれか。

ア：表は必ず画像ファイルだけを保存し、文字や数値は扱えない。

イ：表では全ての行が完全に同一でなければならない。

ウ：表は行と列から構成され、各行がレコード、列が属性に対応する形でデータを表現する。

エ：表はDNS名前解決のためだけに使われる。

答え・解説 正答：ウ

ア：関係データベースは文字・数値など多様なデータを扱えます。

イ：各行は異なるレコードを表せます。

ウ：関係データベースでは表形式でデータを表現し、行と列に意味を持たせます。

エ：データベースの用途はDNSに限定されません。

総合解説：関係データベースは、データを表の行・列として扱うモデルです。キーや関係を利用してデータを整理し、SQLなどで検索・更新します。

対象：2026年度 / 基準日 2026-09-05

0032 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：基礎

SQLの主な用途として、最も適切なものはどれか。

ア：無線LANの電波強度だけを調整する。

イ：メールサーバ間のメッセージ転送だけを行う。

ウ：ルータの物理配線を自動的に変更する。

エ：関係データベースに対するデータの検索、追加、更新、削除や定義などを行う。

答え・解説 正答：エ

ア：SQLは無線LAN制御の言語ではありません。

イ：メール転送はSMTPの役割です。

ウ：SQLはネットワーク配線変更のための言語ではありません。

エ：SQLは関係データベースを操作・定義するために広く用いられる言語です。

総合解説：SQLはデータベース操作の基本です。セキュリティ面では、必要な権限だけを付与し、アプリケーションからの入力を安全に扱うことも重要です。

対象：2026年度 / 基準日 2026-09-05

0033 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：基礎

データベースのアクセス制御として、最も適切なものはどれか。

ア：利用者や役割ごとに業務上必要な権限だけを付与し、不要な参照・更新権限を与えない。

イ：全利用者へ常に管理者権限を付与して運用を簡単にする。

ウ：退職者のアカウントも監査用として無期限に有効のまま残す。

エ：データベースの権限はネットワーク接続の有無だけで決まり、利用者識別は不要である。

答え・解説 正答：ア

ア：最小権限の考え方に基づき、必要な操作だけを許可することが基本です。

イ：過大な権限は誤操作や不正利用の影響を拡大します。

ウ：不要なアカウントは無効化・削除など適切に管理すべきです。

エ：DBでも利用者や役割に応じた認証・認可が重要です。

総合解説：データベースでは、利用者・役割・業務に応じて参照、更新、管理などの権限を制御します。不要な権限を削減することで、誤操作や侵害時の影響を抑えます。

対象：2026年度 / 基準日 2026-09-05

0034 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：標準

銀行振込で「A口座から減額」と「B口座へ加算」を一つの業務処理として扱う。途中で障害が起きた場合の望ましいトランザクション処理はどれか。

ア：A口座の減額だけ成功した状態を必ず確定し、残りは放置する。

イ：一連の更新を整合した単位として扱い、途中失敗なら不完全な更新を残さず元の状態へ戻せるようにする。

ウ：障害の有無にかかわらず全更新を二重に実行する。

エ：DB更新では整合性を考慮せず、画面表示だけを正しく見せればよい。

答え・解説 正答：イ

ア：一連の処理の整合性が崩れます。

イ：関連更新を一つのトランザクションとして扱うことで、中途半端な状態を避けます。

ウ：重複更新は整合性を損なう可能性があります。

エ：表示だけでなく永続データの整合性が必要です。

総合解説：トランザクション処理では、一連の関連更新を整合した単位として管理します。障害時にはコミット前の変更を取り消すなど、データの不整合を防ぐ仕組みが重要です。

対象：2026年度 / 基準日 2026-09-05

0035 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：標準

複数利用者が同じ在庫レコードを同時に更新するシステムで、排他制御を行う主な目的はどれか。

ア：データベースの全データを自動的に公開情報へ変換する。

イ：バックアップ媒体を物理的に廃棄する。

ウ：同時更新の競合によって更新内容が失われたり、不整合が生じたりすることを防ぐ。

エ：SQLを使わずにDNSレコードを更新する。

答え・解説 正答：ウ

ア：排他制御は公開範囲を変更する仕組みではありません。

イ：媒体廃棄は排他制御とは別の運用です。

ウ：排他制御は同時実行による競合を調整し、データ整合性を保つために使われます。

エ：DNS更新はDB排他制御の目的ではありません。

総合解説：同じデータへの並行更新では、更新の消失や不整合が起こり得ます。ロックなどの同時実行制御によって、業務上正しい順序と整合性を確保します。

対象：2026年度 / 基準日 2026-09-05

0036 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：標準

フルバックアップの説明として、最も適切なものはどれか。

ア：前回のバックアップ以降に変更されたデータだけを必ず取得する方式である。

イ：最後のフルバックアップ以降の変更分だけを必ず取得する方式である。

ウ：バックアップを一切取得せず、RAIDだけを利用する方式である。

エ：対象となるデータ一式をバックアップするため、一般に取得量は大きいが、復元の基点として扱いやすい。

答え・解説 正答：エ

ア：これは増分バックアップの説明に近いです。

イ：これは差分バックアップの説明に近いです。

ウ：RAIDはバックアップ方式ではありません。

エ：フルバックアップは対象全体を取得するため容量・時間は増えやすい一方、復元の基礎になります。

総合解説：バックアップ方式は、取得時間、保存容量、復元時間のトレードオフで選びます。フル・差分・増分の違いを理解し、復元手順まで設計します。

対象：2026年度 / 基準日 2026-09-05

0037 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：標準

日曜にフルバックアップを取得し、月曜以降は毎日バックアップする。火曜の増分バックアップで通常取得する対象として最も適切なものはどれか。

ア：月曜のバックアップ以降に変更されたデータ。

イ：日曜のフルバックアップ以降に変更された全データを必ず取得する。

ウ：変更の有無にかかわらず全データを毎回取得する。

エ：データではなくDNSキャッシュだけを取得する。

答え・解説 正答：ア

ア：増分バックアップは直前のバックアップ以降に変更されたデータを取得する考え方です。

イ：これは差分バックアップの考え方に近いです。

ウ：これはフルバックアップです。

エ：DBバックアップの対象説明として不適切です。

総合解説：増分バックアップは直前のバックアップ以降の変更分、差分バックアップは直近フル以降の変更分を取得するのが基本です。復元時に必要な媒体数や時間も異なります。

対象：2026年度 / 基準日 2026-09-05

0038 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：応用

日曜にフル、月曜・火曜・水曜に増分バックアップを取得している。水曜取得後の状態へ復元する基本手順として最も適切なものはどれか。

ア：水曜の増分だけを空のDBへ適用すれば全データが必ず復元できる。

イ：日曜のフルを復元した後、月曜、火曜、水曜の増分を順に適用する。

ウ：日曜フルを復元した後、水曜増分だけを適用し、月曜・火曜を必ず飛ばす。

エ：バックアップは取得するだけでよく、復元手順の確認は不要である。

答え・解説 正答：イ

ア：増分には変更分しか含まれないため、基点となるフル等が必要です。

イ：増分方式ではフルバックアップと、その後の各増分を順に適用するのが基本です。

ウ：増分は連続した変更履歴なので途中を飛ばせません。

エ：復元可能性を確認しなければ、障害時に使えないバックアップとなるリスクがあります。

総合解説：増分バックアップは取得量を抑えやすい一方、復元には連続するバックアップが必要になります。実運用では定期的なリストアテストで手順と所要時間を確認します。

対象：2026年度 / 基準日 2026-09-05

0039 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：応用

昨日のバックアップにも気付かないデータ破損が含まれていた。復旧可能性を高めるバックアップ運用として最も適切なものはどれか。

ア：常に最新1世代だけを上書きし、過去世代は残さない。

イ：RAIDを使っているのでバックアップ世代は不要と判断する。

ウ：複数世代のバックアップを保持し、破損前の時点へ戻せるようにする。

エ：バックアップを本番DBと同じ論理領域だけに置き、アクセス権も全利用者へ付与する。

答え・解説 正答：ウ

ア：破損が最新バックアップにも含まれると戻せる時点がありません。

イ：RAIDは論理破損や誤操作からの時点復旧を代替しません。

ウ：世代管理により、直近バックアップ自体が不適切な場合でも過去時点から復旧できる可能性が高まります。

エ：同時被害や誤削除の影響を受けやすくなります。

総合解説：バックアップは「ある」だけでなく、必要な時点へ戻せることが重要です。世代管理、保管場所、アクセス制御、復元テストを組み合わせて復旧可能性を高めます。

対象：2026年度 / 基準日 2026-09-05

0040 データベース・クラウド > データベース基礎・アクセス制御・バックアップ ｜ 難易度：標準

バックアップ運用の評価として、最も適切なものはどれか。

ア：バックアップジョブが開始したログだけを見れば、復元可能性は100%保証される。

イ：バックアップ媒体は誰でも削除できる共有領域に置く。

ウ：一度成功したら、その後はシステム変更があっても復元テストを永久に省略する。

エ：定期的に復元テストを行い、必要なデータが目標時間内に復旧できるか確認する。

答え・解説 正答：エ

ア：開始ログだけでは完了・完全性・復元可能性を確認できません。

イ：誤削除や侵害のリスクが高まります。

ウ：構成変更やデータ増加により復元手順・時間は変わるため継続的確認が必要です。

エ：バックアップの目的は復元なので、実際の復元可能性と所要時間を確認することが重要です。

総合解説：バックアップは復旧できて初めて有効です。取得結果だけでなく、復元手順、媒体、権限、所要時間を定期的に検証します。

対象：2026年度 / 基準日 2026-09-05

0041 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：基礎

WebブラウザとWebサーバの関係として、最も適切なものはどれか。

ア：WebブラウザがHTTPなどで要求を送り、Webサーバが要求に応じたコンテンツや応答を返す。

イ：Webサーバは常に利用者PCのキーボード入力を物理的に制御する。

ウ：WebブラウザはDNSサーバそのものであり、Webサーバを必要としない。

エ：Webサーバはメール配送専用で、HTTPを処理しない。

答え・解説 正答：ア

ア：ブラウザがクライアント、Webサーバがサーバとして要求・応答を行うのが基本です。

イ：Webサーバはキーボードを物理制御する装置ではありません。

ウ：ブラウザとDNSサーバは異なる役割です。

エ：WebサーバはHTTP等のWeb要求を処理します。

総合解説：Webシステムはクライアントサーバ方式の代表例です。ブラウザ、Webサーバ、必要に応じてアプリケーションやDBが連携して処理します。

対象：2026年度 / 基準日 2026-09-05

0042 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：基礎

利用者がブラウザから特定のWeb資源を指定するときに使うURLの役割として、正しいものはどれか。

ア：LANスイッチのMACアドレス表だけを指す。

イ：Web上の資源の場所やアクセス方法を識別するために用いられる文字列である。

ウ：データベースのバックアップ世代番号だけを指す。

エ：無線LANの暗号鍵だけを指す。

答え・解説 正答：イ

ア：URLとMACアドレス表は別のものです。

イ：URLはWeb資源を識別・参照するために利用され、スキーム、ホスト名、パスなどを含むことがあります。

ウ：URLはバックアップ番号ではありません。

エ：URLはWi-Fi鍵ではありません。

総合解説：URLはWeb資源への参照を表します。利用者が入力したURLからホスト名の名前解決やHTTP要求が行われるため、DNSとWebの役割を関連付けて理解します。

対象：2026年度 / 基準日 2026-09-05

0043 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：基礎

WebにおけるCookieの一般的な用途として、最も適切なものはどれか。

ア：物理サーバへ非常用電力を供給する。

イ：ルータのIP経路表を恒久的に置き換える。

ウ：ブラウザ側に小さな情報を保存し、後続要求で識別子などを送ることで状態管理を補助する。

エ：データベースのフルバックアップを自動取得する。

答え・解説 正答：ウ

ア：Cookieは電源装置ではありません。

イ：Cookieはルーティング制御に使いません。

ウ：HTTP自体はステートレスなので、Cookieはログイン状態などを関連付ける手段の一つとして使われます。

エ：Cookieはバックアップ機能ではありません。

総合解説：Cookieはクライアント側に保存される情報で、サーバ側セッションの識別子などに使われます。機密情報の扱い、Secure等の属性、保存期間などはセキュリティ設計上重要です。

対象：2026年度 / 基準日 2026-09-05

0044 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：標準

Webシステムで、画面表示、業務ロジック、データ保存の役割を分離する利点として、最も適切なものはどれか。

ア：全機能を一つの巨大な処理へ密結合させ、変更時に必ず全体を停止させるため。

イ：Webサーバを使わずに電子メールだけで全処理を実行するため。

ウ：データベースのアクセス制御を不要にするため。

エ：役割ごとに変更や拡張を行いやすくし、保守性やスケーラビリティを高めやすい。

答え・解説 正答：エ

ア：分離の目的と逆です。

イ：Webシステムの役割分離の説明ではありません。

ウ：層分離してもDB権限管理は必要です。

エ：役割を層として分離すると、責務が明確になり変更影響を局所化しやすくなります。

総合解説：Webシステムではプレゼンテーション、アプリケーション、データ層などに責務を分ける構成が一般的です。分離は保守性や拡張性に寄与しますが、各層間の認証・権限・通信も適切に設計します。

対象：2026年度 / 基準日 2026-09-05

0045 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：標準

ログイン後の複数画面で同じ利用者として処理を継続するWebアプリケーションの設計として、最も適切なものはどれか。

ア：HTTP要求は原則独立しているため、セッションIDなどを用いてサーバ側の利用者状態と要求を対応付ける。

イ：HTTPは全利用者のログイン状態をネットワーク全体で永久に自動保持するため、状態管理は不要である。

ウ：DNSのTTLを利用者IDとして使えば、セッション管理になる。

エ：RAIDレベルを変更すればログイン状態を識別できる。

答え・解説 正答：ア

ア：継続状態はHTTP外の仕組みで補う必要があり、Cookieとサーバ側セッションの組合せなどが利用されます。

イ：HTTP自体はステートレスであり、そのような自動保持はしません。

ウ：DNS TTLはキャッシュ期間であり、利用者セッション識別に使うものではありません。

エ：RAIDはストレージ構成であり、Webセッション識別とは無関係です。

総合解説：Webアプリケーションは、ステートレスなHTTP上で状態を継続するための仕組みを設計します。セッションIDの推測防止、期限、ログアウト時の無効化なども重要です。

対象：2026年度 / 基準日 2026-09-05

0046 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：標準

商品検索Webシステムで、ブラウザから受けた検索条件を基にDBへ問い合わせ、結果をHTMLとして返す構成の説明として最も適切なものはどれか。

ア：L2スイッチがSQLを生成してDB更新を行うのが標準である。

イ：Webアプリケーションが要求を解釈してDBへ問い合わせ、Webサーバを通じて結果を利用者へ返す。

ウ：UPSがHTMLを生成して検索結果を返す。

エ：DNSサーバが全商品の在庫を必ず保持し、DBは不要である。

答え・解説 正答：イ

ア：L2スイッチはネットワークフレーム転送が主な役割です。

イ：Webアプリケーションは利用者要求とDB処理の仲介・業務ロジックを担います。

ウ：UPSは電源装置です。

エ：DNSは名前解決用であり、商品DBの代替ではありません。

総合解説：Webシステムでは、Webサーバ、アプリケーション、DBがそれぞれの役割を分担します。障害や性能問題の切分けでも、どの層で処理が滞っているかを区別します。

対象：2026年度 / 基準日 2026-09-05

0047 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：標準

Webフォームの入力チェックをブラウザ側JavaScriptだけで実施している。改善として最も適切なものはどれか。

ア：JavaScriptがあるので、サーバはどの入力値でも無条件に受け入れる。

イ：入力値の検証をDNSへ委任する。

ウ：ブラウザ側のチェックに加え、サーバ側でも入力値を検証し、不正な要求をそのまま信用しない。

エ：DBのバックアップ頻度を上げれば、入力検証は不要になる。

答え・解説 正答：ウ

ア：攻撃者はブラウザ側検証を迂回できるため危険です。

イ：DNSはWeb入力検証のための仕組みではありません。

ウ：クライアント側処理は利用者に変更・回避され得るため、サーバ側検証が必要です。

エ：バックアップと入力検証は目的が異なります。

総合解説：Webアプリケーションでは、クライアント側の入力支援は利便性向上に使えますが、信頼境界はサーバ側です。サーバ側で型、範囲、長さ、許可形式などを検証します。

対象：2026年度 / 基準日 2026-09-05

0048 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：応用

Webページの静的画像は表示できるが、商品検索だけが「DB接続失敗」と表示される。最初に重点確認すべき対象はどれか。

ア：全社WAN回線が完全に断線していると断定する。

イ：利用者のディスプレイ故障だけを疑う。

ウ：SSIDの表示名だけを変更する。

エ：WebアプリケーションからDBへの接続設定、DBサービス稼働状態、認証情報など。

答え・解説 正答：エ

ア：静的画像が同じWebサイトから表示できるなら、全経路断と断定できません。

イ：DB接続失敗というサーバ側メッセージと整合しません。

ウ：DB接続障害の第一の対策ではありません。

エ：静的コンテンツ配信は動いているため、アプリケーションからDBまでの経路を重点確認するのが合理的です。

総合解説：Webシステムの障害切分けでは、静的配信、アプリケーション、DBなど処理層を分けて考えます。一部機能だけが失敗している場合、共通して正常な層を除外して原因範囲を絞ります。

対象：2026年度 / 基準日 2026-09-05

0049 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：応用

セッション情報を各Webアプリケーションサーバのメモリだけに保持している。負荷分散で複数サーバへ要求を振り分ける際の課題として最も適切なものはどれか。

ア：要求が別サーバへ振り分けられると、そのサーバにセッション情報がなく利用者状態を継続できない可能性がある。

イ：サーバを複数にするとHTTPが必ず使えなくなる。

ウ：負荷分散を導入するとDNSが物理的に消滅する。

エ：複数サーバではデータベースを一切利用できない。

答え・解説 正答：ア

ア：ローカルメモリだけのセッションはサーバ間で共有されないため、負荷分散時に状態管理の設計が必要です。

イ：複数サーバでもHTTPは利用できます。

ウ：負荷分散導入とDNSの存在は別です。

エ：複数サーバから共有DBへ接続する構成は一般的です。

総合解説：ステートフルなアプリケーションを複数サーバへ分散する場合、セッション共有、外部セッションストア、スティッキーセッションなどの設計が必要です。可用性と拡張性を考えて状態の置き場所を決めます。

対象：2026年度 / 基準日 2026-09-05

0050 データベース・クラウド > Webシステム・アプリケーション基礎 ｜ 難易度：標準

HTMLとHTTPの関係として、最も適切な説明はどれか。

ア：HTMLはIP経路制御プロトコルで、HTTPはストレージ冗長化方式である。

イ：HTMLはWeb文書の構造を記述するためのマークアップ言語で、HTTPはWeb資源を要求・応答でやり取りするためのプロトコルである。

ウ：HTMLとHTTPは同一のものを別表記しただけである。

エ：HTTPはDBのバックアップ形式で、HTMLはメール配送プロトコルである。

答え・解説 正答：イ

ア：どちらの説明も誤りです。

イ：HTMLとHTTPはそれぞれ文書表現と言語通信という異なる役割を持ちます。

ウ：文書記述と通信プロトコルで役割が異なります。

エ：どちらも用途が異なります。

総合解説：Webの基本要素は役割で整理すると理解しやすくなります。HTMLはコンテンツ構造、HTTPは通信、URLは資源参照、DNSは名前解決を担います。

対象：2026年度 / 基準日 2026-09-05

0051 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：基礎

利用部門が自前でOSやアプリケーションを構築せず、事業者が提供する完成済み業務ソフトをネットワーク経由で使う形態はどれか。

ア：利用者が物理サーバのCPUを製造するサービスモデルである。

イ：利用者が必ずハイパーバイザから全て管理するサービスモデルである。

ウ：クラウド事業者が提供するアプリケーションを、利用者がネットワーク経由で利用するサービスモデルである。

エ：インターネットを使わないローカル紙文書管理だけを指す。

答え・解説 正答：ウ

ア：SaaSはハードウェア製造モデルではありません。

イ：これはSaaSの責任範囲とは異なります。

ウ：SaaSでは利用者は提供済みアプリケーションを利用し、基盤やOSの管理は通常クラウド事業者側が担います。

エ：SaaSはクラウドサービスモデルです。

総合解説：SaaSは完成したソフトウェア機能をサービスとして利用するモデルです。メール、グループウェア、CRMなどが例になり得ます。

対象：2026年度 / 基準日 2026-09-05

0052 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：基礎

開発チームが自作アプリを配置したい一方、OSや実行基盤の運用はクラウド事業者へ任せたい。この提供形態の説明として正しいものはどれか。

ア：完成した業務アプリケーションだけを利用し、アプリ配置は一切行わないモデルに限定される。

イ：仮想マシンやストレージなど基盤資源だけを主に提供するモデルである。

ウ：DNSキャッシュだけを提供するモデルである。

エ：利用者がアプリケーションを開発・配置するための実行環境やプラットフォームをサービスとして利用するモデルである。

答え・解説 正答：エ

ア：これはSaaSの説明に近いです。

イ：これはIaaSの説明に近いです。

ウ：PaaSはDNSキャッシュだけに限定されません。

エ：PaaSではOS等の基盤管理を事業者に任せつつ、利用者がアプリケーションを展開できます。

総合解説：PaaSはアプリケーションの開発・実行に必要なプラットフォームを提供します。利用者はアプリ開発へ注力できる一方、提供環境の制約や設定責任を理解して利用します。

対象：2026年度 / 基準日 2026-09-05

0053 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：基礎

クラウド上で仮想マシンやストレージを確保し、利用者側でOSやアプリケーションを管理する利用形態を正しく説明したものはどれか。

ア：仮想マシン、ストレージ、ネットワークなどの基盤資源をサービスとして利用し、利用者がOSやアプリケーションを管理する範囲が比較的大きい。

イ：利用者は完成済みアプリの画面だけ使い、OSやアプリ設定には一切関与しないモデルだけを指す。

ウ：利用者がクラウド事業者の物理データセンター設備を必ず自分で保守する。

エ：IaaSではネットワーク資源を利用できない。

答え・解説 正答：ア

ア：IaaSはインフラ資源を提供し、利用者はOS以上の層を管理することが一般的です。

イ：これはSaaSに近い説明です。

ウ：物理基盤は通常事業者が管理します。

エ：IaaSにはネットワークなどの基盤資源も含まれます。

総合解説：IaaSは利用者の自由度が高い一方、OS設定、パッチ、アプリ、アカウントなど利用者側の管理範囲も大きくなります。サービスモデルごとの責任範囲を理解します。

対象：2026年度 / 基準日 2026-09-05

0054 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：標準

自社で開発したWebアプリケーションを配置したいが、OSのパッチ適用やミドルウェア基盤の管理はできるだけ事業者へ任せたい。選択肢として最も適切なのはどれか。

ア：SaaSだけ。

イ：PaaS。

ウ：IaaSだけ。

エ：LANスイッチ。

答え・解説 正答：イ

ア：既製アプリの利用が中心で、自社アプリの任意配置という要件に必ずしも合いません。

イ：PaaSはアプリケーションの配置・実行環境を提供し、基盤管理を事業者へ任せやすいモデルです。

ウ：IaaSでは利用者がOS等を管理する範囲が通常PaaSより広くなります。

エ：LANスイッチはクラウドサービスモデルではありません。

総合解説：クラウド選定では「何を自社で管理したいか」を明確にします。アプリ開発は自社、OS等の基盤運用は事業者へ寄せたい場合、PaaSが候補になります。

対象：2026年度 / 基準日 2026-09-05

0055 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：標準

NISTが示すクラウドの「オンデマンドセルフサービス」の説明として、最も適切なものはどれか。

ア：資源追加のたびに必ず紙の申請書を郵送し、数週間の手作業を要する。

イ：全利用者が同じ固定容量を永久に使い続け、変更できない。

ウ：利用者が必要に応じて、事業者担当者との都度の人的やり取りを要せず計算資源などを自動的に確保できる。

エ：クラウドでは利用量を把握できないことを意味する。

答え・解説 正答：ウ

ア：オンデマンドな自動提供とは逆の性質です。

イ：必要に応じた迅速な資源調達という特性に合いません。

ウ：オンデマンドセルフサービスは、必要な資源を利用者自身が迅速に調達できる特性です。

エ：利用量の計測は別の基本特性です。

総合解説：クラウドの基本特性にはオンデマンドセルフサービス、広範なネットワークアクセス、資源プーリング、迅速な伸縮性、計測可能なサービスがあります。用語だけでなく意味を区別します。

対象：2026年度 / 基準日 2026-09-05

0056 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：標準

繁忙時間だけサーバ資源を増やし、需要が下がれば短時間で減らせるクラウドの特性として、最も適切なものはどれか。

ア：データの世代管理。

イ：メールリレー。

ウ：排他制御。

エ：迅速な伸縮性（rapid elasticity）。

答え・解説 正答：エ

ア：バックアップ運用の概念で、クラウドの伸縮性を表しません。

イ：電子メール転送の仕組みです。

ウ：DB同時実行制御の概念です。

エ：需要に応じて資源を迅速に拡大・縮小できることがクラウドの主要特性です。

総合解説：クラウドは需要変動へ追随して資源を増減しやすい点が特徴です。ただし自動スケールの条件、上限、コスト、アプリ側の対応可否は設計時に確認します。

対象：2026年度 / 基準日 2026-09-05

0057 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：標準

クラウドの「資源プーリング」に関する説明として、最も適切なものはどれか。

ア：事業者の計算・ストレージ等の資源を共有プールとして管理し、需要に応じて複数利用者へ動的に割り当てる。

イ：利用者ごとに必ず専用の物理データセンターを新築することだけを意味する。

ウ：全利用者のデータをアクセス制御せず同一ファイルとして混在させることを意味する。

エ：ネットワークを使わず、紙帳票だけを共同利用することを意味する。

答え・解説 正答：ア

ア：資源プーリングは共有基盤から利用者へ資源を割り当てるクラウドの基本特性です。

イ：資源プーリングの説明ではありません。

ウ：論理的分離やアクセス制御を無視する意味ではありません。

エ：クラウド資源プーリングの説明ではありません。

総合解説：クラウドでは共有インフラを効率的に利用しつつ、利用者間を論理的に分離します。共有であることと、無制限に他利用者のデータへアクセスできることは別です。

対象：2026年度 / 基準日 2026-09-05

0058 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：応用

クラウド利用料をCPU時間、保存容量、通信量などの実績に応じて集計している。この性質に最も対応するクラウドの基本特性はどれか。

ア：排他制御。

イ：計測可能なサービス（measured service）。

ウ：DNS名前解決。

エ：ホットスタンバイ。

答え・解説 正答：イ

ア：DB同時実行制御の概念です。

イ：クラウドでは資源利用を計測・監視し、利用者と事業者の双方が利用状況を把握できる特性があります。

ウ：名前とアドレスの対応付けであり、利用量計測ではありません。

エ：待機系構成の方式であり、クラウド利用量の計測特性ではありません。

総合解説：計測可能なサービスは、従量課金だけでなく容量管理やコスト最適化にも関係します。利用部門はメトリクスを確認し、想定外の利用増加や不要資源を管理します。

対象：2026年度 / 基準日 2026-09-05

0059 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：応用

SaaSへ移行したため「情報セキュリティ管理は全て事業者に移った」と担当者が主張した。評価として最も適切なものはどれか。

ア：適切である。SaaSでは利用者側のアクセス権設定は存在しない。

イ：適切である。クラウドではデータの分類やバックアップ要件を検討してはいけない。

ウ：不適切である。SaaSでも利用者アカウント、権限、保存するデータ、設定、利用ルールなど利用組織側に残る管理責任がある。

エ：不適切だが、理由はSaaSではネットワークを一切利用しないからである。

答え・解説 正答：ウ

ア：SaaSでも利用者・権限管理は通常必要です。

イ：利用データの重要度や復旧要件は利用組織が把握すべきです。

ウ：SaaSで基盤管理の多くを委ねても、利用者側のID・データ・設定・運用責任まで消えるわけではありません。

エ：SaaSは通常ネットワーク経由で利用します。

総合解説：クラウドは管理責任を分担するサービスです。サービスモデルにより事業者と利用者の担当範囲は変わりますが、利用組織のデータ・ID・アクセス・設定管理などは残ります。

対象：2026年度 / 基準日 2026-09-05

0060 データベース・クラウド > SaaS・PaaS・IaaS・クラウド利用 ｜ 難易度：標準

クラウドの「広範なネットワークアクセス」の説明として、最も適切なものはどれか。

ア：クラウドは必ず専用端末1台からしか使えないことを意味する。

イ：クラウドではネットワークを利用せず、物理媒体の手渡しだけで提供することを意味する。

ウ：利用者が他利用者の全データへ自由にアクセスできることを意味する。

エ：標準的な仕組みを通じてネットワーク越しにサービスへアクセスでき、PCやモバイル端末など多様なクライアントから利用できる性質を指す。

答え・解説 正答：エ

ア：広範なアクセスとは逆です。

イ：クラウドのネットワークアクセス特性に反します。

ウ：アクセス範囲の広さと権限分離は別の概念です。

エ：クラウドサービスはネットワーク経由で幅広いクライアントから利用できることが基本特性の一つです。

総合解説：クラウドはネットワークを通じて利用できる利便性があります。一方で、どこからでもアクセス可能になり得るため、認証、端末管理、アクセス条件などを適切に設計します。

対象：2026年度 / 基準日 2026-09-05

0061 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：基礎

外部のITサービスを利用する契約で、月間可用性や問い合わせ応答時間を双方の評価基準として明確にしたい。この目的に用いるものはどれか。

ア：サービス提供者と顧客の間で、提供するサービス水準や評価指標などについて合意した内容を文書化したものである。

イ：システムの全ソースコードを必ず公開するための文書である。

ウ：従業員の給与額だけを定める文書である。

エ：DBの主キーを一覧化する技術文書だけを指す。

答え・解説 正答：ア

ア：SLAはサービスレベルに関する合意を明確にし、測定・評価の基準とします。

イ：SLAの目的はソースコード公開ではありません。

ウ：サービス水準の合意とは無関係です。

エ：SLAはデータモデル文書ではありません。

総合解説：SLAではサービス時間、応答時間、可用性など、顧客にとって意味のあるサービス水準を明確にします。合意した指標を継続的に測定・報告し、必要に応じて改善します。

対象：2026年度 / 基準日 2026-09-05

0062 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：基礎

サービスレベル目標の設定例として、最も適切なものはどれか。

ア：「できるだけ頑張る」のように測定方法を定めない。

イ：「月間可用性99.9%以上」のように、対象期間と測定可能な指標を明確にする。

ウ：「絶対に障害を起こさない」とだけ書き、対象範囲も計測方法も決めない。

エ：技術担当者の感想だけを唯一の評価指標にする。

答え・解説 正答：イ

ア：達成度を客観評価できません。

イ：サービスレベルは測定・評価できる形で定義することが重要です。

ウ：実務的に評価できる目標になっていません。

エ：客観的なサービス指標が必要です。

総合解説：サービスレベル管理では、何を、どの期間、どの方法で測るかを明確にします。可用性、応答時間、サービス時間、問い合わせ応答などが指標候補になります。

対象：2026年度 / 基準日 2026-09-05

0063 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：基礎

サービスカタログの主な役割として、最も適切なものはどれか。

ア：ネットワーク機器のMACアドレスだけを永久保存する。

イ：バックアップ媒体を物理的に破壊する手順だけをまとめる。

ウ：利用可能なITサービスの内容、対象、条件などを整理し、利用者や管理者がサービスを把握できるようにする。

エ：DNSのTTLだけを変更するためのファイルである。

答え・解説 正答：ウ

ア：MAC表だけを扱うものではありません。

イ：サービスカタログの目的ではありません。

ウ：サービスカタログは提供サービスを体系的に整理し、サービス管理の基礎情報とします。

エ：サービスカタログはDNS設定ファイルではありません。

総合解説：サービスカタログは「どのサービスを、誰に、どの条件で提供しているか」を理解するための基盤です。SLA、サービス要求、構成情報と関連付けて管理します。

対象：2026年度 / 基準日 2026-09-05

0064 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：標準

外部クラウド事業者へ重要システムの一部を委託している。供給者管理として最も適切なものはどれか。

ア：契約締結後は供給者の実績を一切確認しない。

イ：供給者に任せた部分は自社サービスのSLA評価から必ず除外する。

ウ：障害時の連絡先や責任範囲を契約に書かない。

エ：自社サービスの要求事項と整合するよう契約・サービス水準を定め、実績を継続的に監視・評価する。

答え・解説 正答：エ

ア：サービス水準の継続管理ができません。

イ：顧客へのサービス責任と外部供給者の利用は別であり、整合を取る必要があります。

ウ：障害対応の遅延や責任不明確化につながります。

エ：外部供給者のサービスも自社のサービスレベル達成に影響するため、契約と実績管理が必要です。

総合解説：供給者管理では、外部サービスが自社のサービス要求を支えられるかを確認します。契約、SLA、連絡体制、実績報告、改善要求などを継続的に管理します。

対象：2026年度 / 基準日 2026-09-05

0065 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：標準

SLAで「月間可用性99.9%以上」と合意している。サービスレベル管理として最も適切な運用はどれか。

ア：合意した定義と測定方法に基づいて月間実績を算出し、目標未達時は原因と改善策を確認する。

イ：可用性を測定せず、担当者の印象だけで達成とする。

ウ：障害があった月は測定対象から自動的に除外する。

エ：SLA締結後は目標値を確認しない。

答え・解説 正答：ア

ア：SLAは合意した指標を測定・報告し、未達を改善につなげるために利用します。

イ：客観的な達成度を判断できません。

ウ：合意した除外条件がない限り恣意的な除外は適切ではありません。

エ：継続的なサービスレベル管理になりません。

総合解説：SLAは契約書を作ることが目的ではなく、サービスを測定・評価・改善するための基準です。定義の一貫性とデータの信頼性も重要です。

対象：2026年度 / 基準日 2026-09-05

0066 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：標準

「平日9時〜18時にサービスを提供し、画面操作への平均応答時間は2秒以内」と定めている。二つの指標の対応として最も適切なものはどれか。

ア：9時〜18時はMTBF、2秒以内はRPOである。

イ：9時〜18時はサービス時間、2秒以内は応答時間に関する目標である。

ウ：9時〜18時はRTO、2秒以内はバックアップ世代である。

エ：両方ともDNS TTLだけを表している。

答え・解説 正答：イ

ア：いずれも異なる概念です。

イ：サービス時間は提供する時間帯、応答時間は要求から応答までの時間を表します。

ウ：RTOや世代管理の説明ではありません。

エ：DNS TTLとは無関係です。

総合解説：サービスレベルでは複数の指標を混同しないことが重要です。提供時間帯、可用性、応答時間、問い合わせ対応などを個別に定義・測定します。

対象：2026年度 / 基準日 2026-09-05

0067 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：標準

顧客には24時間365日のサービスと短い復旧時間を約束しているが、主要外部供給者との契約は平日日中のみサポートである。最も適切な対応はどれか。

ア：供給者契約は顧客SLAと無関係なので何も確認しない。

イ：顧客SLAを実現できないことを把握していても、供給者へ一切伝えない。

ウ：顧客へのサービスレベルを支えられるよう、供給者との契約・サポート条件や代替策を見直す。

エ：SLAの測定を停止すれば不整合は解消する。

答え・解説 正答：ウ

ア：供給者障害が自社サービスへ影響するため無関係ではありません。

イ：サービス提供能力の不整合を放置すべきではありません。

ウ：上位の顧客要求を満たすには、依存する供給者の条件と整合を取る必要があります。

エ：問題を測定しないことは解決ではありません。

総合解説：サービスチェーンでは、外部供給者の契約条件が顧客向けSLAを支えられるか確認します。不足があれば契約、冗長化、代替供給者、内部運用などを見直します。

対象：2026年度 / 基準日 2026-09-05

0068 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：応用

SLAの可用性目標は達成しているが、利用者から「問い合わせへの返答が遅い」という不満が増えている。最も適切な対応はどれか。

ア：可用性が達成しているため、利用者の不満は必ず無視する。

イ：問い合わせ内容を全て障害として扱い、根本原因分析を禁止する。

ウ：SLAを廃止し、測定を全て停止する。

エ：可用性だけで十分とせず、問い合わせ応答など利用者体験に関する指標やサービス要求を見直す。

答え・解説 正答：エ

ア：顧客満足やサービス要求の変化を無視すべきではありません。

イ：問い合わせにはサービス要求などもあり、分類して管理する必要があります。

ウ：改善のための測定基準を失います。

エ：サービス品質は単一指標だけでは捉えられず、顧客満足や他のサービスレベルも評価すべきです。

総合解説：サービスマネジメントでは、SLA達成だけでなく顧客満足や実際の利用体験も確認します。指標が顧客価値を十分表しているかを定期的に見直します。

対象：2026年度 / 基準日 2026-09-05

0069 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：応用

外部供給者の障害が自社サービスに直結する。供給者管理で事前に定める事項として最も適切なものはどれか。

ア：障害時の連絡窓口、通知期限、エスカレーション、復旧情報の共有方法などを契約・運用手順で明確にする。

イ：連絡先は障害が起きてから初めて探す。

ウ：供給者が障害を公表するまで自社は監視を一切しない。

エ：責任範囲を曖昧にすることで柔軟性を高める。

答え・解説 正答：ア

ア：外部供給者障害時に迅速に連携できるよう、責任と情報共有手順を事前に定めます。

イ：初動が遅れ、顧客対応にも影響します。

ウ：自社でもサービス影響を監視し、必要な連携を行うべきです。

エ：障害時の責任不明確化につながります。

総合解説：供給者管理は平常時の価格・契約管理だけではありません。インシデント時に必要な情報が適時届き、自社の顧客対応へつなげられる体制を準備します。

対象：2026年度 / 基準日 2026-09-05

0070 サービスマネジメント > SLA・サービスレベル・供給者管理 ｜ 難易度：標準

アクセス増加により応答時間のSLA違反が発生し始めた。サービスマネジメント上の対応として最も適切なものはどれか。

ア：応答時間を測定することを停止し、違反が見えないようにする。

イ：CPU、メモリ、ディスク、ネットワーク利用率などを監視し、需要と容量の傾向から増強や最適化を検討する。

ウ：全ての利用者へ管理者権限を付与して処理を高速化する。

エ：DNS名を毎日変更すればCPU不足が解消する。

答え・解説 正答：イ

ア：サービス改善につながりません。

イ：需要管理・容量管理はサービスレベルを維持するために資源使用量と傾向を管理します。

ウ：セキュリティリスクを増やし、容量問題の適切な対策ではありません。

エ：DNS名変更はCPU容量不足を解消しません。

総合解説：サービスレベルの性能目標を守るには、需要とシステム容量の関係を継続的に監視します。閾値や傾向を用いて、問題が顕在化する前に資源計画へ反映します。

対象：2026年度 / 基準日 2026-09-05

0071 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：基礎

サービスマネジメントにおけるインシデント管理の主な目的として、最も適切なものはどれか。

ア：全ての障害について必ず最初に長期間の根本原因研究を完了してから復旧する。

イ：構成情報を削除して障害原因を分からなくする。

ウ：中断・品質低下したサービスをできるだけ早く通常状態へ戻し、業務影響を小さくする。

エ：利用者からの連絡を受け付けない。

答え・解説 正答：ウ

ア：根本原因分析は問題管理の重要な役割で、復旧を不必要に遅らせるべきではありません。

イ：構成情報は切分けや影響評価に役立ちます。

ウ：インシデント管理では迅速なサービス復旧を優先します。

エ：インシデントの受付・記録は重要です。

総合解説：インシデント管理はサービスの早期復旧を中心にします。一方、繰り返す障害の根本原因を分析・除去するのは問題管理の役割です。

対象：2026年度 / 基準日 2026-09-05

0072 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：基礎

問題管理の主な目的として、最も適切なものはどれか。

ア：利用者のパスワードを全員同じに統一する。

イ：障害記録を消去して発生件数を少なく見せる。

ウ：全てのサービス要求を障害と同一扱いし、分類しない。

エ：インシデントの根本原因を分析し、再発防止や影響低減のための恒久対策につなげる。

答え・解説 正答：エ

ア：問題管理の目的ではなく、セキュリティ上不適切です。

イ：傾向分析や改善ができなくなります。

ウ：サービス要求とインシデントは区別して管理します。

エ：問題管理は根本原因、既知の誤り、回避策、傾向分析などを扱います。

総合解説：問題管理は、復旧後も残る根本原因を特定し、再発を防ぐためのプロセスです。インシデント管理と連携しつつ目的を区別します。

対象：2026年度 / 基準日 2026-09-05

0073 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：基礎

構成管理におけるCI（構成品目）の説明として、最も適切なものはどれか。

ア：サービス提供に必要で、管理対象として識別・記録するハードウェア、ソフトウェア、文書などの構成要素である。

イ：インシデント発生時だけ一時的に付ける利用者の感想である。

ウ：可用性を表す百分率そのものである。

エ：DNSのTTLだけを指す略語である。

答え・解説 正答：ア

ア：CIはサービスを構成する管理対象で、属性や関係を把握することが重要です。

イ：CIは管理対象の構成要素です。

ウ：可用性指標とCIは別です。

エ：CIはDNS TTLの略ではありません。

総合解説：構成管理ではCIとその関係を把握し、変更・障害時の影響分析に利用します。情報が古いと誤った判断につながるため、変更と同期して更新します。

対象：2026年度 / 基準日 2026-09-05

0074 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：標準

障害原因の修正には時間がかかるため、サービスを復旧するまで一時的に別サーバへ切り替えて利用を継続した。この一時的な方法の位置付けとして最も適切なものはどれか。

ア：恒久対策が完了したとみなし、原因調査を禁止する。

イ：回避策として利用し、根本原因の分析と恒久対策は問題管理で継続する。

ウ：構成管理情報を削除して切替えを記録しない。

エ：回避策を実施したらインシデントの記録自体を消去する。

答え・解説 正答：イ

ア：再発する可能性があるため問題管理を継続すべきです。

イ：回避策は影響を軽減・回避する一時的な手段で、根本原因の除去とは区別します。

ウ：変更・構成の追跡性を損ないます。

エ：履歴は傾向分析や監査に有用です。

総合解説：迅速な復旧のための回避策と、原因を除去する恒久対策は分けて考えます。回避策を知識化して再利用しつつ、問題管理で根本原因を解消します。

対象：2026年度 / 基準日 2026-09-05

0075 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：標準

原因が特定され、暫定的な回避策も分かっているが、恒久修正はまだ実施していない問題の扱いとして最も適切なものはどれか。

ア：原因が分かっているので記録を削除する。

イ：回避策を担当者個人だけが記憶し、共有しない。

ウ：既知の誤りとして記録し、インシデント対応時に回避策を活用できるようにする。

エ：恒久修正がない限り、利用者へのサービス復旧を禁止する。

答え・解説 正答：ウ

ア：恒久修正まで管理を続ける必要があります。

イ：知識が共有されず復旧時間が長くなります。

ウ：根本原因と回避策が分かっている問題は既知の誤りとして管理し、早期復旧に役立てます。

エ：回避策で安全に復旧できる場合は、影響低減に活用できます。

総合解説：既知の誤り情報は、同じ障害の再発時に迅速に回避策を適用するための知識になります。恒久対策の進捗と併せて管理します。

対象：2026年度 / 基準日 2026-09-05

0076 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：標準

本番サーバのOS更新を計画している。変更管理として最も適切なものはどれか。

ア：影響評価をせず、担当者が思い付いた時間に本番へ適用する。

イ：変更前後の構成情報を記録しない。

ウ：失敗時の切戻し方法を検討しない。

エ：影響範囲、リスク、実施手順、切戻し手順、承認、実施日時などを事前に評価・計画する。

答え・解説 正答：エ

ア：予期せぬ停止や互換性問題のリスクが高まります。

イ：構成管理との整合が取れなくなります。

ウ：復旧不能や停止長期化につながります。

エ：変更によるサービスへの影響を把握し、統制された手順で実施することが変更管理の基本です。

総合解説：変更管理では、必要性とリスクを評価して適切に承認し、実施後も結果を確認します。緊急変更でも記録・権限・事後レビューなど統制を保ちます。

対象：2026年度 / 基準日 2026-09-05

0077 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：標準

重大脆弱性への緊急対応で本番変更が必要になった。最も適切な考え方はどれか。

ア：緊急性に応じて簡略化した承認経路を用いても、変更内容、責任者、影響、結果を記録し、事後レビューを行う。

イ：緊急なら誰でも無記録で本番設定を変更してよい。

ウ：緊急変更は永続的に構成管理の対象外にする。

エ：緊急変更では切戻しを考えてはいけない。

答え・解説 正答：ア

ア：緊急変更でも完全な無統制にせず、迅速さと追跡性を両立します。

イ：無許可・無記録変更は障害や不正の原因になります。

ウ：実施後の構成情報更新が必要です。

エ：失敗時の復旧手段を検討することが重要です。

総合解説：変更管理は速度を落とすことが目的ではなく、変更リスクを統制する仕組みです。緊急時にも必要最小限の承認・記録・確認を残します。

対象：2026年度 / 基準日 2026-09-05

0078 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：応用

共通DBサーバの変更前に、そのサーバへ依存する業務サービスを特定したい。最も有効な情報はどれか。

ア：担当者の記憶だけに依存し、記録は確認しない。

イ：CI間の依存関係を含む、最新の構成管理情報。

ウ：利用者のパスワード一覧。

エ：前年の広告資料だけ。

答え・解説 正答：イ

ア：属人的で漏れや古い情報のリスクがあります。

イ：構成管理で依存関係を把握していれば、変更や障害の影響範囲を分析できます。

ウ：依存サービスの特定に使う情報ではありません。

エ：技術構成の最新依存関係を保証しません。

総合解説：構成管理は資産一覧だけでなく、CI間の関係を把握することに価値があります。変更、インシデント、問題管理で影響分析を支援します。

対象：2026年度 / 基準日 2026-09-05

0079 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：応用

全社基幹システムが停止し、復旧見込みも不明である。サービスデスク担当者の初動として最も適切なものはどれか。

ア：担当者一人で原因が完全に分かるまで誰にも連絡しない。

イ：インシデント記録を作らず、口頭だけで処理する。

ウ：重大度基準に従って速やかにエスカレーションし、専門担当・責任者を招集しつつ利用者への状況連絡を行う。

エ：停止が重大であるほど利用者への状況連絡を禁止する。

答え・解説 正答：ウ

ア：復旧・意思決定・利用者連絡が遅れます。

イ：追跡・共有・後日の分析ができません。

ウ：重大インシデントは通常の処理だけに留めず、権限・専門性を持つ関係者へ迅速に引き上げます。

エ：適切な状況共有は混乱低減に重要です。

総合解説：重大インシデントでは、技術対応と同時に組織的なエスカレーション、意思決定、コミュニケーションが必要です。重大度基準と連絡経路を平常時から定めます。

対象：2026年度 / 基準日 2026-09-05

0080 サービスマネジメント > インシデント・問題・変更・構成管理 ｜ 難易度：標準

利用者から「承認済みの標準ソフトウェアを新PCへインストールしてほしい」という依頼が来た。障害や品質低下は発生していない。最も適切な分類はどれか。

ア：必ず重大インシデントとして扱う。

イ：根本原因がある問題として必ず扱う。

ウ：構成管理を廃止する理由として扱う。

エ：サービス要求として扱う。

答え・解説 正答：エ

ア：サービス停止や品質低下がないため重大インシデントではありません。

イ：通常の標準依頼であり、問題管理の対象とは限りません。

ウ：ソフト導入はむしろ構成情報更新の対象になり得ます。

エ：定型的な情報・アクセス・標準作業の依頼は、障害復旧を目的とするインシデントと区別して管理します。

総合解説：受付時にインシデント、サービス要求、問題などを適切に分類すると、優先度や処理手順を標準化できます。要求完了後は必要に応じて構成情報も更新します。

対象：2026年度 / 基準日 2026-09-05

0081 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：基礎

災害対策会議で「基幹サービスは停止から4時間以内に再開する」と決めた。この4時間が表す指標はどれか。

ア：障害や災害の発生後、対象サービスを復旧させるまでの目標時間である。

イ：許容できるデータ損失量を時間で示す指標だけを指す。

ウ：平均故障間隔を示す指標である。

エ：DNSキャッシュの保持時間である。

答え・解説 正答：ア

ア：RTOはサービスやシステムをどれだけの時間内に復旧するかを示す目標です。

イ：これはRPOの説明に近いです。

ウ：平均故障間隔はMTBFです。

エ：DNS TTLとは別の指標です。

総合解説：RTOは復旧に要する時間の目標です。重要業務ほど短いRTOが求められることがありますが、短縮には冗長化や待機系などのコストが伴います。

対象：2026年度 / 基準日 2026-09-05

0082 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：基礎

災害対策会議で「障害時に失ってよい更新データは最大30分分まで」と決めた。この30分が主に表す指標はどれか。

ア：サービスを復旧するまでの目標時間だけを示す。

イ：障害時にどの時点までのデータを復旧できればよいかを示し、許容するデータ損失の時間幅に関係する目標である。

ウ：システムの平均故障間隔を示す。

エ：Web画面の平均応答時間を示す。

答え・解説 正答：イ

ア：これはRTOの説明です。

イ：RPOは復旧対象とするデータ時点を表し、バックアップや複製の頻度設計に影響します。

ウ：これはMTBFです。

エ：性能指標でありRPOではありません。

総合解説：RPOは「どこまでデータを戻せればよいか」を時間軸で表します。RTOとRPOは別指標なので、業務影響分析に基づいてそれぞれ設定します。

対象：2026年度 / 基準日 2026-09-05

0083 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：基礎

サービス可用性管理の考え方として、最も適切なものはどれか。

ア：障害記録を削除して可用性が高く見えるようにする。

イ：バックアップを取得したら可用性測定を永久に止める。

ウ：合意したサービス時間や可用性目標を満たせるよう、障害・復旧・冗長性などを継続的に管理する。

エ：利用者数が増えるほど、必ず可用性は100%になるとみなす。

答え・解説 正答：ウ

ア：実態を隠すだけで改善になりません。

イ：バックアップと可用性測定は別です。

ウ：可用性管理はサービスが必要なときに利用できる状態を維持・改善する活動です。

エ：利用者数だけで可用性は決まりません。

総合解説：可用性管理は故障の発生頻度だけでなく、復旧時間、冗長構成、保守性、運用手順などを総合的に扱います。実績を測定し、サービスレベルと比較して改善します。

対象：2026年度 / 基準日 2026-09-05

0084 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：標準

業務上のRPOが1時間である。データ更新が継続するシステムのバックアップ設計として、最も適切な考え方はどれか。

ア：毎日1回だけバックアップすれば、どの時刻の障害でも必ずRPO1時間を満たす。

イ：RPOは復旧にかかる作業時間だけなので、バックアップ頻度と無関係である。

ウ：RPOを短くするにはDNS TTLだけを短くすればよい。

エ：最大1時間を超えるデータ損失にならないよう、バックアップやレプリケーションの間隔・方式を設計する。

答え・解説 正答：エ

ア：最悪24時間近いデータ損失が発生し得ます。

イ：RPOは復旧可能なデータ時点に関係します。

ウ：DNS TTLはデータ保護間隔を決めません。

エ：RPOは許容するデータ損失幅なので、保護方式の実効間隔が目標を支える必要があります。

総合解説：RPOを満たすには、バックアップやレプリケーションによって失われる可能性のある更新量を制限します。実際の取得成功率や復元可能性も検証します。

対象：2026年度 / 基準日 2026-09-05

0085 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：標準

停止後30分以内の復旧が必要な重要サービスについて、数日かけて機器を調達・構築する方式では要件を満たせない。最も適切な改善方向はどれか。

ア：ホットスタンバイなど、短いRTOを支えられる待機・冗長構成を検討する。

イ：RTOを無視し、障害時に初めて機器購入を検討する。

ウ：バックアップを廃止して復旧作業を減らす。

エ：サービス停止を測定しなければRTOを満たしたことにする。

答え・解説 正答：ア

ア：短いRTOには事前に準備された復旧資源や自動・迅速な切替えが必要になることがあります。

イ：30分の要件を満たせません。

ウ：データ復旧能力を失うため不適切です。

エ：測定を止めても実際の停止時間は変わりません。

総合解説：RTOが短いほど、ホットスタンバイ、クラスタ、レプリケーションなど平常時の投資が必要になりやすくなります。業務影響とコストを踏まえて方式を選びます。

対象：2026年度 / 基準日 2026-09-05

0086 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：標準

複数業務のRTO・RPOを決める際の進め方として、最も適切なものはどれか。

ア：全業務のRTO・RPOを根拠なく同じ値にする。

イ：業務停止やデータ損失が与える影響をBIAで評価し、重要度と許容限界に基づいてRTO・RPOを設定する。

ウ：バックアップ装置の型番だけを見てRTOを決める。

エ：障害が一度も起きていなければRTO・RPOは不要とする。

答え・解説 正答：イ

ア：業務重要度や許容停止時間は異なるため合理的ではありません。

イ：復旧目標は技術部門の都合だけでなく、業務影響から導くことが重要です。

ウ：業務要件を先に把握する必要があります。

エ：発生前に継続要件を定めて準備することが重要です。

総合解説：BIAは業務停止・データ損失の影響と時間的な許容度を明確にします。その結果を復旧優先順位やRTO/RPO、復旧資源の設計へ反映します。

対象：2026年度 / 基準日 2026-09-05

0087 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：標準

月30日（720時間）のうち、対象サービスが計3.6時間停止した。単純に「稼働時間÷総サービス時間」で可用性を求めると、最も適切な値はどれか。

ア：0.5%。停止時間だけを総時間で割った値を可用性とする。

イ：50%。停止時間が1時間を超えたため一律50%とする。

ウ：99.5%。稼働時間716.4時間を720時間で割る。

エ：100%。月末に復旧していれば停止時間は無視する。

答え・解説 正答：ウ

ア：3.6/720=0.5%は停止率であり、可用性ではありません。

イ：そのような計算方法ではありません。

ウ：716.4÷720=0.995なので99.5%です。

エ：実際に停止した時間を考慮します。

総合解説：可用性はSLAの代表的指標です。計算時にはサービス時間、計画停止の扱い、測定点など、SLAで合意した定義を一貫して適用します。

対象：2026年度 / 基準日 2026-09-05

0088 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：応用

災害復旧計画を作成したが、5年間一度も訓練しておらず、担当者やシステム構成も変わっている。最も適切な対応はどれか。

ア：計画書が存在するので、訓練しなくても必ず復旧できると判断する。

イ：担当者変更があるほど、計画書を古い状態のまま固定する。

ウ：復旧訓練で問題が見つかる可能性があるため、テストを禁止する。

エ：計画を現状に合わせて更新し、定期的な訓練・テストで復旧手順とRTO/RPO達成可能性を確認する。

答え・解説 正答：エ

ア：実際の連絡先・権限・構成が変われば計画が機能しない可能性があります。

イ：現状と不一致になり、復旧失敗の原因になります。

ウ：問題を事前に発見・改善することが訓練の目的です。

エ：継続計画は文書化だけでなく、環境変化に合わせた保守と演習が必要です。

総合解説：サービス継続計画は、組織・システムの変更に合わせて保守し、演習によって実効性を確認します。机上演習、技術復旧テスト、総合訓練などを目的に応じて行います。

対象：2026年度 / 基準日 2026-09-05

0089 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：応用

受注システムで「障害発生から2時間以内にサービス再開」「失ってよい受注データは最大15分分まで」と業務部門が要求した。対応する指標の組合せとして最も適切なものはどれか。

ア：RTOは2時間（サービス再開までの目標時間）、RPOは15分（許容できるデータ損失の時間幅）と設定する。

イ：RTOを15分のデータ損失許容量、RPOを2時間のサービス復旧時間として扱い、二つの指標の意味を逆にする。

ウ：MTBFを2時間、MTTRを15分と読み替え、RTOとRPOは設定しない。

エ：SLAは不要とし、DNS TTLを2時間に設定することで復旧時間とデータ損失の双方を管理する。

答え・解説 正答：ア

ア：サービス再開までの目標時間がRTO、許容できるデータ損失の時間幅がRPOなので、要求に対応しています。

イ：RTOは復旧時間、RPOは許容データ損失の時間幅であり、二つの意味が逆です。

ウ：MTBF・MTTRは故障間隔・修復時間の指標であり、提示された事業継続要求をそのまま置き換えるものではありません。

エ：DNS TTLだけでは復旧時間と許容データ損失の要件を管理できません。

総合解説：RTOとRPOは混同しやすい指標です。サービス復旧の速さと、復旧できるデータ時点を別々に設計し、双方を満たす技術・運用を選びます。

対象：2026年度 / 基準日 2026-09-05

0090 サービスマネジメント > 可用性・継続管理・RTO・RPO ｜ 難易度：標準

本番サーバとバックアップサーバを同じラック、同じ電源系統に置いている。拠点停電への継続対策として最も適切な評価はどれか。

ア：サーバが2台あるので、同じ電源でも停電の影響を必ず受けない。

イ：共通の電源・場所が単一障害点になり得るため、必要なRTO/RPOに応じて別電源系統や別拠点などの分離を検討する。

ウ：同じラックに置くほど地震・火災への耐性が必ず高くなる。

エ：バックアップサーバがある場合、RTO/RPOを決める必要はない。

答え・解説 正答：イ

ア：共通電源障害では2台とも停止し得ます。

イ：同じ災害要因で本番と待機系が同時に失われる構成では継続性が不足する可能性があります。

ウ：共通災害の影響範囲を広げる可能性があります。

エ：復旧目標は業務要件として定める必要があります。

総合解説：冗長化では「同じ原因で同時に失われないか」を確認します。機器だけ二重化しても、電源、回線、建物などが共通なら単一障害点が残ります。

対象：2026年度 / 基準日 2026-09-05

0091 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：基礎

プロジェクトの説明として、最も適切なものはどれか。

ア：特定の目的を達成するために期間を定めて実施され、固有の成果物や結果を生み出す活動である。

イ：日常業務と同じ手順を期限なく反復する活動だけを指す。

ウ：組織図上の部門を新設することだけを指し、成果物は必要ない。

エ：障害対応のように開始時点も終了条件も定めない活動を指す。

答え・解説 正答：ア

ア：プロジェクトは、目的・期間・成果が明確な一時的な取組として管理します。

イ：反復的な定常業務は運用として扱われるのが一般的で、プロジェクトとは区別します。

ウ：組織変更がプロジェクトの一部になることはありますが、部門新設だけが定義ではありません。

エ：終了条件を定めず継続する活動はプロジェクトの基本的特徴と合いません。

総合解説：情報セキュリティ施策でも、認証基盤導入や規程改定などは期限と成果物を定めたプロジェクトとして進めることがあります。運用との違いを押さえることが重要です。

対象：2026年度 / 基準日 2026-09-05

0092 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：基礎

全社の認証基盤更改プロジェクトで、経営方針との整合や重要な意思決定の責任を明確にしたい。最も適切な対応はどれか。

ア：担当者ごとに独自ルールで意思決定し、全体の承認経路は設けない。

イ：プロジェクトガバナンスとして意思決定権限、報告経路、責任を定め、組織の目的との整合を確認する。

ウ：技術者だけで全社方針を変更できるようにし、経営層への報告を省く。

エ：日々の作業記録だけを残し、プロジェクト目的との整合は確認しない。

答え・解説 正答：イ

ア：意思決定がばらばらになると統制が効かず、重要事項の責任も不明確になります。

イ：ガバナンスは、責任・権限・監督の仕組みを通じてプロジェクトを組織目的に整合させます。

ウ：全社方針に関わる判断を技術担当だけに委ねるのは適切ではありません。

エ：作業記録は必要ですが、目的・方針との整合確認の代わりにはなりません。

総合解説：プロジェクトマネジメントでは作業管理だけでなく、誰が何を決め、どこへ報告し、組織戦略とどう整合させるかというガバナンスも重要です。

対象：2026年度 / 基準日 2026-09-05

0093 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：基礎

顧客情報を扱う新システムの導入計画を立てている。ステークホルダの特定として最も適切なものはどれか。

ア：プロジェクトマネージャだけをステークホルダとし、利用者は含めない。

イ：契約前は委託先候補を一切考慮せず、内部関係者だけに限定する。

ウ：利用部門、システム部門、情報セキュリティ部門、経営層、必要に応じ委託先など、影響を受ける又は影響を与える関係者を洗い出す。

エ：意思決定権のない利用者は影響を受けてもステークホルダから除外する。

答え・解説 正答：ウ

ア：プロジェクトマネージャは重要な関係者ですが、それだけでは不足します。

イ：調達や連携が予定される場合、外部関係者の影響も検討対象になります。

ウ：ステークホルダは、プロジェクトに影響する又は影響を受ける関係者を幅広く特定します。

エ：利用者は要件や受入れに大きく関わるため、意思決定権が弱くても重要なステークホルダです。

総合解説：ステークホルダを早期に特定すると、要件漏れ、合意不足、導入後の反発などを減らせます。情報セキュリティ部門も早期に関与させることが有効です。

対象：2026年度 / 基準日 2026-09-05

0094 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：標準

WBS（Work Breakdown Structure）の利用目的として最も適切なものはどれか。

ア：サーバのIPアドレスを自動配布する。

イ：監査ログを時系列に暗号化する。

ウ：組織の貸借対照表を作成する。

エ：プロジェクトのスコープを管理可能な作業単位へ階層的に分解し、作業の抜けや範囲を把握しやすくする。

答え・解説 正答：エ

ア：IPアドレスの自動配布はDHCPなどの役割です。

イ：ログ暗号化はWBSの目的ではありません。

ウ：貸借対照表は会計上の財務諸表であり、WBSとは異なります。

エ：WBSは成果や作業を階層的に分解し、スコープや見積り、担当割当ての基礎にします。

総合解説：セキュリティ施策でも、設計、構築、テスト、教育、移行などの作業をWBSで分解すると、必要作業の漏れを発見しやすくなります。

対象：2026年度 / 基準日 2026-09-05

0095 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：標準

プロジェクトで複数のリスクが特定された。限られた資源で対応の優先順位を決める考え方として最も適切なものはどれか。

ア：発生可能性と影響度などを評価し、重大なリスクから対応を検討する。

イ：すべてのリスクを発生可能性に関係なく同じ優先度にする。

ウ：金額に換算できないリスクは必ず無視する。

エ：発生後に初めてリスク一覧を作り、それまでは記録しない。

答え・解説 正答：ア

ア：リスクは特定後に評価し、発生可能性や影響などを踏まえて優先順位を付けます。

イ：重要度に差があるため、すべて同列では資源配分が非効率になります。

ウ：信用失墜や法令違反など、金額化が難しい重大影響もあります。

エ：事前に特定・評価して備えることがリスクマネジメントの目的です。

総合解説：プロジェクトリスクでは、単に一覧を作るだけでなく、評価、対応、監視まで継続します。セキュリティリスクもプロジェクトリスクの一部として扱えます。

対象：2026年度 / 基準日 2026-09-05

0096 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：標準

開発中、利用部門から当初要件にない監査レポート機能の追加要望が出た。最も適切な対応はどれか。

ア：要望を受けた担当者の判断だけで即日追加し、計画や契約は変更しない。

イ：影響するコスト、納期、品質、セキュリティを評価し、定めた変更管理手続に従って承認可否を決める。

ウ：追加要望はすべて拒否し、事業上の必要性は確認しない。

エ：本番リリース後に利用者へ知らせればよいので、影響評価は不要とする。

答え・解説 正答：イ

ア：無断追加はスコープ拡大や納期遅延、品質低下につながります。

イ：変更は影響を評価し、承認された変更として計画やベースラインへ反映します。

ウ：変更を一律拒否すると必要な事業要件を満たせない可能性があります。

エ：変更前に影響を把握して意思決定する必要があります。

総合解説：変更管理は、変更を禁止する仕組みではなく、変更の必要性と影響を見える化し、統制された意思決定を行う仕組みです。

対象：2026年度 / 基準日 2026-09-05

0097 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：標準

プロジェクト終結時の活動として、今後のセキュリティ施策にも役立つ最も適切なものはどれか。

ア：完了したら関連記録をすべて削除し、振り返りを行わない。

イ：問題があっても責任追及を避けるため記録しない。

ウ：成功要因、問題、対応結果などの教訓を整理し、再利用できる形で組織に共有する。

エ：成果物の受入れ確認をせず、予定日になった時点で自動的に終結する。

答え・解説 正答：ウ

ア：必要な記録の保存や教訓管理を行わないと、同じ失敗を繰り返しやすくなります。

イ：問題と対策を事実ベースで記録することは組織学習に有用です。

ウ：終結では成果確認とともに教訓を収集し、次のプロジェクトへ活かします。

エ：受入れや残課題の確認なしの終結は適切ではありません。

総合解説：教訓は個人の記憶に留めず、再利用可能な知識として残すことが重要です。セキュリティ事故やテストで得た知見も次回計画へ反映します。

対象：2026年度 / 基準日 2026-09-05

0098 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：標準

重大な仕様変更について、複数部門の責任者間でその場で質疑し合意形成する必要がある。最も適切なコミュニケーション方法はどれか。

ア：共有フォルダに資料だけ置き、閲覧したかを確認しない。

イ：一方向の一斉メールだけを送り、質問は受け付けない。

ウ：関係者には知らせず、作業完了後に結果だけ公開する。

エ：会議やオンライン会議などの双方向コミュニケーションを用い、論点を確認しながら合意する。

答え・解説 正答：エ

ア：共有フォルダはプル型情報提供に向きますが、緊急の合意形成には不十分な場合があります。

イ：一方向通知は情報配布には使えますが、質疑を伴う合意形成には弱い方法です。

ウ：重要変更を事前共有しないと、手戻りや対立の原因になります。

エ：複雑で合意が必要な事項は、即時に質問・回答できる双方向コミュニケーションが適します。

総合解説：プロジェクトでは、情報の重要度、緊急度、受け手、合意の必要性に応じて、双方向・プッシュ型・プル型などを使い分けます。

対象：2026年度 / 基準日 2026-09-05

0099 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：応用

認証基盤更改で、A「主要製品の納入遅延：発生可能性高・影響大」、B「会議室不足：発生可能性中・影響小」が特定された。対応として最も適切なものはどれか。

ア：Aを高優先度で扱い、代替調達やスケジュール見直しなどの対応策を検討し、Bは相対的に低い優先度で管理する。

イ：Bだけを優先し、Aは納入日になるまで何もしない。

ウ：発生可能性と影響を比較せず、名称の長いリスクから対処する。

エ：AとBの情報を削除し、リスクが存在しない前提で基準計画を維持する。

答え・解説 正答：ア

ア：発生可能性と影響がともに大きいAは優先して対応すべきリスクです。

イ：Aの方がプロジェクト目標への影響が大きく、後回しは不適切です。

ウ：リスク名の表現は優先度の根拠になりません。

エ：特定済みリスクを無視すると、予防・軽減の機会を失います。

総合解説：リスク評価は、対応資源の優先配分に使います。評価基準を定め、対応後も残留リスクや状況変化を監視することが重要です。

対象：2026年度 / 基準日 2026-09-05

0100 プロジェクト・調達 > プロジェクト管理・リスク・ステークホルダ ｜ 難易度：応用

新サービスの開発で、情報セキュリティ部門は本番直前の検査だけ参加すればよいという案が出た。最も適切な評価はどれか。

ア：本番直前までセキュリティ要求を定めない方が、必ず開発コストは下がる。

イ：要件や設計段階からセキュリティ部門を関与させ、重大な要求漏れを早期に発見した方が手戻りを減らしやすい。

ウ：セキュリティ部門が参加すると機能要件を一切決められなくなるため、終盤だけでよい。

エ：セキュリティは運用開始後に追加すれば十分で、受入れ条件には含めない。

答え・解説 正答：イ

ア：後から重大な設計変更が必要になると、むしろコストや納期への影響が大きくなります。

イ：セキュリティ要求は後付けより早期に整理した方が、設計・契約・テストへ反映しやすくなります。

ウ：セキュリティ部門は機能要件を妨げる存在ではなく、リスクと要求の整合を支援します。

エ：運用後追加だけでは、構造的な弱点や受入れ基準漏れが残るおそれがあります。

総合解説：ステークホルダ管理では、必要な専門家を適切な時期に関与させることが重要です。セキュリティ・バイ・デザインの観点からも早期関与は有効です。

対象：2026年度 / 基準日 2026-09-05

0101 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：基礎

要件定義の説明として最も適切なものはどれか。

ア：プログラムの全ソースコードを確定する活動だけを指す。

イ：サーバのラック内配線だけを決める活動である。

ウ：業務上必要な機能、品質、セキュリティ、データなどについて、システムが満たすべき要求を明確にする活動である。

エ：導入後の障害記録だけを集計する活動である。

答え・解説 正答：ウ

ア：ソースコードは実装段階の成果物で、要件定義そのものではありません。

イ：配線設計は実現手段の一部であり、要件定義より下流の具体化です。

ウ：要件定義では、何を満たすべきかを整理し、設計や調達の基礎にします。

エ：障害記録集計は運用・改善に関する活動です。

総合解説：セキュリティ要求も機能要件や非機能要件と同様に、設計・テスト・契約へつながる形で明確化する必要があります。

対象：2026年度 / 基準日 2026-09-05

0102 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：基礎

次のうち、セキュリティに関する非機能要件の例として最も適切なものはどれか。

ア：受注登録画面で商品コードと数量を入力できるようにする。

イ：利用者が注文内容を検索できるようにする。

ウ：請求書PDFを出力する機能を追加する。

エ：管理者ログインには多要素認証を要求し、認証失敗を監査ログへ記録する。

答え・解説 正答：エ

ア：受注登録は業務機能に関する機能要件です。

イ：注文検索も業務機能に関する要件です。

ウ：帳票出力もシステムが提供する機能要件です。

エ：認証強度やログ記録は、システムの品質・制約に関するセキュリティ要求として扱われます。

総合解説：要件定義では、機能要件だけでなく、性能、可用性、セキュリティなどの非機能要件も明確にします。

対象：2026年度 / 基準日 2026-09-05

0103 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：基礎

セキュリティ要求事項として、受入れ時に検証しやすい記述はどれか。

ア：管理者アカウントは多要素認証を必須とし、認証失敗記録を180日以上検索可能な状態で保存する。

イ：できるだけ安全な認証にする。

ウ：必要に応じて十分なログを残す。

エ：担当者が不安を感じない程度に保護する。

答え・解説 正答：ア

ア：対象、条件、保存期間などが具体的で、テストや監査で確認しやすい要求です。

イ：「できるだけ安全」は評価基準が曖昧で、合否を判定できません。

ウ：「必要に応じて」「十分な」は解釈が分かれやすい表現です。

エ：利用者の主観だけでは技術的・運用的な受入れ基準になりません。

総合解説：良い要求事項は、関係者が同じ意味に解釈でき、実装後に満たしたか検証できることが重要です。

対象：2026年度 / 基準日 2026-09-05

0104 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：標準

要求事項と設計・テストの対応関係を追跡できるようにする主な利点として最も適切なものはどれか。

ア：要求が未実装でも自動的に合格扱いにできる。

イ：各要求が設計やテストに反映されたか確認しやすくなり、変更時の影響範囲も追跡しやすい。

ウ：要件変更の影響分析が不要になる。

エ：関係者の承認や受入れ試験を省略できる。

答え・解説 正答：イ

ア：未実装要求を合格扱いにするための仕組みではありません。

イ：トレーサビリティにより、要求から実装・テストまでのつながりを確認できます。

ウ：むしろ変更時の影響分析を支援するために有効です。

エ：承認や受入れの代替ではなく、確認を支える情報です。

総合解説：セキュリティ要求は漏れが重大事故につながるため、要求IDなどを使って設計・テストケースと対応付けると管理しやすくなります。

対象：2026年度 / 基準日 2026-09-05

0105 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：標準

社外秘情報を扱うシステムと、公開情報だけを扱う広報サイトで同一のセキュリティ要求を機械的に適用しようとしている。最も適切な考え方はどれか。

ア：情報の種類に関係なく、すべて最低限の対策だけにそろえる。

イ：公開情報サイトの要件を基準にし、機密情報システムにもそのまま適用する。

ウ：扱う情報の重要度、脅威、利用形態、法令・契約条件などを踏まえてリスクを評価し、必要な要求を決める。

エ：セキュリティ要件はコストしか考えず、情報価値や脅威は考慮しない。

答え・解説 正答：ウ

ア：重要情報を扱うシステムに最低限の対策だけでは不足する場合があります。

イ：機密性や規制要件の差を無視すると必要な保護が欠けます。

ウ：セキュリティ要求は、対象システムのリスクと事業要件に応じて定めます。

エ：コストは重要ですが、リスクを無視して要件を決めるのは不適切です。

総合解説：同じ組織でもシステムごとに情報価値や脅威は異なります。リスクベースで要求の強度を決めることが合理的です。

対象：2026年度 / 基準日 2026-09-05

0106 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：標準

受注停止が長引くと大きな損失が出るシステムの要件定義で、可用性に関して最も適切な対応はどれか。

ア：可用性は設計者の感覚だけで決め、業務部門には確認しない。

イ：バックアップが存在すれば停止時間の要件は不要とする。

ウ：可用性要件は本番障害が起きた後に初めて決める。

エ：業務が許容できる停止時間や復旧目標を明確にし、それを満たす冗長化・バックアップ・運用要件へつなげる。

答え・解説 正答：エ

ア：技術部門だけで決めると業務の許容範囲とずれる可能性があります。

イ：バックアップの有無だけでは復旧時間を保証できません。

ウ：障害前に要求を定めて設計・テストへ反映する必要があります。

エ：可用性は業務影響と復旧目標を踏まえて要件化します。

総合解説：要件定義では、障害時に何時間で再開すべきかなど、業務側の期待を検証可能な形へ落とし込むことが重要です。

対象：2026年度 / 基準日 2026-09-05

0107 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：標準

顧客情報システムのアクセス制御要件として、最小権限の考え方に最も合うものはどれか。

ア：職務に必要な範囲だけ参照・更新権限を付与し、異動や退職時には権限を見直す。

イ：全社員に管理者権限を付与し、使わないよう教育だけ行う。

ウ：一度付与した権限は業務が変わっても削除しない。

エ：共有管理者IDを全員で使い、利用者を識別しない。

答え・解説 正答：ア

ア：必要最小限の権限を付与し、職務変更に応じて見直すことが最小権限の原則です。

イ：過剰権限は誤操作や不正利用時の被害を拡大します。

ウ：職務変更後の不要権限は残存リスクになります。

エ：共有IDは誰が操作したか追跡しにくく、説明責任を損ないます。

総合解説：セキュリティ要件は、認証方式だけでなく、誰がどのデータへ何をできるかという認可の範囲まで具体化する必要があります。

対象：2026年度 / 基準日 2026-09-05

0108 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：標準

要件定義で、個人情報と公開情報を同じ保護レベルで扱う案がある。最も適切な対応はどれか。

ア：データ分類は不要とし、すべてのデータを公開情報として扱う。

イ：データの種類や重要度を分類し、保存・転送・アクセス・廃棄などに必要な保護要件を分類に応じて定める。

ウ：保存時の保護だけ決め、転送や廃棄は考慮しない。

エ：利用者が自由に保護レベルを変更できるようにし、承認を不要とする。

答え・解説 正答：イ

ア：個人情報などを公開情報扱いにすると過小保護になります。

イ：データ分類は、保護レベルを合理的に決める基礎になります。

ウ：データはライフサイクル全体で保護する必要があります。

エ：保護レベルの変更は統制された手続で行うべきです。

総合解説：情報・データ要件とセキュリティ要件は分離せず、どのデータを誰がどこでどう扱うかまで結び付けて整理します。

対象：2026年度 / 基準日 2026-09-05

0109 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：応用

外部開発するWebシステムのRFPにセキュリティ要求を記載する。受入れ条件として最も適切なものはどれか。

ア：「安全なシステムであること」とだけ記載し、判定方法はベンダーに一任する。

イ：受入れ試験では画面デザインだけを確認し、セキュリティは対象外とする。

ウ：要求した認証・権限制御・ログ・脆弱性対策について、具体的な試験方法と合否基準を定め、受入れ時に確認できるようにする。

エ：契約後に初めて重要なセキュリティ要求を追加し、費用や納期への影響は考慮しない。

答え・解説 正答：ウ

ア：抽象的な表現では、発注者とベンダーで完成条件の認識がずれるおそれがあります。

イ：セキュリティ要件も受入れ対象として確認すべきです。

ウ：要件と受入れ基準を対応付けると、納品時に満たしているか客観的に確認できます。

エ：後付け要求は紛争や追加費用の原因となるため、可能な限り早期に明確化します。

総合解説：調達案件では、要求事項をRFPや契約条件へ落とし、テスト可能な受入れ基準まで整合させることが重要です。

対象：2026年度 / 基準日 2026-09-05

0110 プロジェクト・調達 > 要件定義・セキュリティ要求事項 ｜ 難易度：応用

要件確定後、新たな規制対応によりログ保存要件を強化する必要が判明した。最も適切な対応はどれか。

ア：確定済み要件は理由に関係なく絶対に変更しない。

イ：担当者が設計書だけ修正し、要件書やテスト仕様は更新しない。

ウ：新要件を口頭だけで伝え、承認記録は残さない。

エ：変更理由を記録し、設計・テスト・費用・納期への影響を分析した上で、正式な変更手続によって要求を更新する。

答え・解説 正答：エ

ア：法令・事業・リスク変化に応じた必要変更まで禁止するのは不合理です。

イ：要件と設計・テストの不整合が生じます。

ウ：口頭だけでは合意内容や責任が追跡できません。

エ：要件確定後でも必要な変更はあり得るため、影響を分析し統制された変更として処理します。

総合解説：変更管理では、要件・設計・テスト・契約など関連成果物を一貫して更新し、トレーサビリティを維持することが重要です。

対象：2026年度 / 基準日 2026-09-05

0111 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：基礎

RFI（Request For Information）の主な目的として最も適切なものはどれか。

ア：調達の初期段階で、候補となる製品・サービス・技術やベンダーの情報を広く収集する。

イ：最終的な発注契約を締結する。

ウ：納品物の検収を完了させる。

エ：ベンダーへ確定済み仕様に対する正式な提案と見積を必ず提出させる。

答え・解説 正答：ア

ア：RFIは情報提供依頼であり、市場や選択肢を把握するために使います。

イ：契約締結はRFIそのものの目的ではありません。

ウ：検収は調達後の受入れ段階で行います。

エ：具体的な提案依頼はRFP、見積依頼はRFQなどが適します。

総合解説：RFI、RFP、RFQは目的が異なります。RFIで情報収集し、要求を具体化してRFPやRFQへ進む流れを理解します。

対象：2026年度 / 基準日 2026-09-05

0112 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：基礎

RFP（Request For Proposal）の説明として最も適切なものはどれか。

ア：社内の障害対応手順だけを記載する文書である。

イ：発注側が目的、対象範囲、要件、スケジュール、契約条件などを示し、ベンダーに具体的な提案を求める文書である。

ウ：会計年度末の財務諸表をベンダーへ提出する文書である。

エ：受注後の作業日報だけを収集する文書である。

答え・解説 正答：イ

ア：障害対応手順書とは目的が異なります。

イ：RFPは、発注側の要求を示し、ベンダーから実現方法や体制、費用などの提案を得るために使います。

ウ：財務諸表の提出文書ではありません。

エ：作業日報は契約履行中の管理資料で、RFPではありません。

総合解説：RFPの内容が曖昧だと提案比較が難しくなるため、対象範囲や評価に必要な条件を明確にすることが重要です。

対象：2026年度 / 基準日 2026-09-05

0113 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：基礎

仕様や数量がほぼ確定しており、複数ベンダーから価格条件を比較するため見積を求めたい。最も適切な文書はどれか。

ア：RFI（Request For Information）

イ：WBS（Work Breakdown Structure）

ウ：RFQ（Request For Quotation）

エ：BIA（Business Impact Analysis）

答え・解説 正答：ウ

ア：RFIは市場・技術・製品などの情報収集が中心です。

イ：WBSはプロジェクト作業を分解する管理手法です。

ウ：RFQは見積依頼書であり、価格や条件の提示を求める場面で用います。

エ：BIAは事業中断の影響を分析する活動です。

総合解説：RFI＝情報収集、RFP＝提案依頼、RFQ＝見積依頼という違いを整理すると、調達プロセスを理解しやすくなります。

対象：2026年度 / 基準日 2026-09-05

0114 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：標準

複数ベンダーの提案を公平に比較したい。RFPに含める内容として最も適切なものはどれか。

ア：発注側の要求は示さず、各ベンダーに自由形式で全て決めてもらう。

イ：価格だけを求め、性能・セキュリティ・体制・実績は比較しない。

ウ：評価基準は選定後に作り、提案前には一切整理しない。

エ：対象範囲、必要機能・サービス要件、目標スケジュール、契約条件、評価に必要な提出事項を明示する。

答え・解説 正答：エ

ア：前提が揃わないと提案内容を横並びで比較しにくくなります。

イ：価格だけでは品質・リスク・要求適合度を評価できません。

ウ：評価基準は提案受領前に整理しておく方が公正性と一貫性を確保しやすくなります。

エ：比較可能性を高めるには、各社が同じ前提で提案できるよう要求と提出条件を明確にします。

総合解説：RFPは単なる製品カタログ依頼ではなく、発注側の要求と評価に必要な情報を構造化して伝える文書です。

対象：2026年度 / 基準日 2026-09-05

0115 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：標準

顧客情報システムのベンダー選定で、最も適切な評価方法はどれか。

ア：要求事項適合度、技術力、実績、プロジェクト体制、セキュリティ、費用、スケジュールなどを事前に定めた基準で総合評価する。

イ：最安値であれば要件未達でも必ず採用する。

ウ：営業担当者の印象だけで決め、提案書は確認しない。

エ：選定基準を提案開封後に都合よく変更する。

答え・解説 正答：ア

ア：ベンダー選定は価格だけでなく、要求適合性や遂行能力を含めて評価します。

イ：要件未達では安価でも事業目的を達成できない可能性があります。

ウ：印象だけでは客観性や説明可能性が不足します。

エ：後から基準を変えると選定の公平性・一貫性が損なわれます。

総合解説：セキュリティを重視する案件では、過去実績、体制、脆弱性対応、インシデント時の連絡なども評価項目として具体化します。

対象：2026年度 / 基準日 2026-09-05

0116 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：標準

システム開発委託で、発注者とベンダーの責任の認識違いによるトラブルを減らす対応として最も適切なものはどれか。

ア：責任分担は書面化せず、その都度口頭で決める。

イ：要件確定、データ提供、テスト、受入れ、障害対応などの役割分担と責任を契約・付属文書で明確にする。

ウ：発注者側の協力事項は一切定めず、全責任をベンダーに負わせる。

エ：ベンダー側の作業範囲を定めず、必要になった作業は無制限に追加する。

答え・解説 正答：イ

ア：口頭だけでは後から認識を確認しにくくなります。

イ：役割と責任を事前に明確化すると、期待のずれや未実施作業を減らせます。

ウ：発注者にも要件提示や受入れなどの協力責任が生じる場合があります。

エ：範囲不明確な契約は費用・納期・品質の紛争要因になります。

総合解説：IPAのモデル取引・契約書も、ユーザ企業とITベンダが各段階で担う責務を明確にし、共通理解を形成することを重視しています。

対象：2026年度 / 基準日 2026-09-05

0117 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：標準

納品後に「完成したかどうか」で争いにならないため、契約前に定める事項として最も適切なものはどれか。

ア：完成条件は定めず、ベンダーが完成と宣言した日を自動的に検収日とする。

イ：成果物一覧を作らず、何が納品されるかは終了時に決める。

ウ：成果物、受入れ基準、受入れ試験の方法、受入れ時期などを明確にする。

エ：受入れ試験は不要とし、要件への適合確認を行わない。

答え・解説 正答：ウ

ア：一方的な宣言だけでは要求適合の確認になりません。

イ：成果物が不明確だと完成範囲を判断できません。

ウ：受入れ条件を具体化すると、納品物が契約上の要求を満たすか共通基準で確認できます。

エ：受入れ確認を省くと要件未達を見逃すおそれがあります。

総合解説：要件定義、RFP、契約、受入れ試験の内容を一貫させることで、調達の品質を高められます。

対象：2026年度 / 基準日 2026-09-05

0118 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：標準

契約後に大規模な追加要件が発生した。最も適切な対応はどれか。

ア：当初契約を変えず、追加作業を無償で行うよう一方的に求める。

イ：担当者同士の口頭合意だけで進め、記録を残さない。

ウ：追加要件の影響を確認せず、元の納期と費用が必ず守られるとみなす。

エ：作業範囲、費用、納期、責任への影響を評価し、変更手続と合意内容を記録して契約・計画を必要に応じ更新する。

答え・解説 正答：エ

ア：一方的な要求は紛争や品質低下の原因になり得ます。

イ：口頭だけでは変更内容や責任の追跡が困難です。

ウ：範囲拡大が納期・費用へ影響しないとは限りません。

エ：大きな変更は契約条件やプロジェクト計画へ影響するため、正式に評価・合意します。

総合解説：変更管理と契約管理を連動させ、合意した範囲と実作業を一致させることが重要です。

対象：2026年度 / 基準日 2026-09-05

0119 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：応用

外部開発したシステムを将来別ベンダーで保守する可能性がある。契約時の確認として最も適切なものはどれか。

ア：成果物の知的財産権、ソースコード等の利用範囲、第三者ソフトウェアのライセンス条件などを確認し、必要な権利を契約で明確にする。

イ：費用を払えば全ての第三者ライセンス条件は自動的に無効になるとみなす。

ウ：知的財産権はシステム運用に影響しないため、契約では扱わない。

エ：将来の保守方法に関係なく、ソースコードやドキュメントの利用条件は確認しない。

答え・解説 正答：ア

ア：利用・改変・保守に必要な権利が確保されているか、契約段階で確認することが重要です。

イ：第三者ライセンスは契約や費用支払だけで消滅するものではありません。

ウ：権利関係は保守・改変・再利用に直接影響します。

エ：将来保守を想定するなら、必要な成果物と利用権の確認が不可欠です。

総合解説：調達では機能・価格だけでなく、知的財産、ライセンス、再委託、保守引継ぎなど将来運用に効く条件も確認します。

対象：2026年度 / 基準日 2026-09-05

0120 プロジェクト・調達 > RFI・RFP・ベンダー選定・契約 ｜ 難易度：応用

クラウドサービスを外部調達する。将来のサービス終了やベンダー変更に備える契約条件として最も適切なものはどれか。

ア：終了時のデータ移行は考えず、サービス内にしか読めない形式でも問題ないとする。

イ：データ返却・移行の方法、利用可能な形式、終了時の削除、引継ぎ、期限や費用などを事前に確認する。

ウ：契約終了後もベンダーがデータを無期限保有できる前提とする。

エ：サービス停止時の連絡や引継ぎ条件を一切定めない。

答え・解説 正答：イ

ア：移行不能な形式はベンダーロックインや業務継続上の問題になります。

イ：出口条件を事前に定めると、ベンダー変更や契約終了時の事業・情報セキュリティリスクを下げられます。

ウ：不要となったデータの扱いは契約・法令・セキュリティ要件に沿って管理すべきです。

エ：終了時の連絡・引継ぎが未定だと停止影響を大きくするおそれがあります。

総合解説：調達は導入時だけでなく、変更・終了までのライフサイクルを考えて契約条件を設計することが重要です。

対象：2026年度 / 基準日 2026-09-05

0121 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：基礎

情報システム戦略の策定で最も重要な考え方はどれか。

ア：最新技術を導入すること自体を最終目的とし、事業課題は確認しない。

イ：各部門が互いに無関係なシステムを自由に導入し、全社方針は持たない。

ウ：経営戦略や事業課題と整合させ、IT投資が事業目標の達成にどう寄与するかを明確にする。

エ：導入費用だけで判断し、効果やリスクは評価しない。

答え・解説 正答：ウ

ア：技術導入は手段であり、事業価値との関係が必要です。

イ：全社整合がないと重複投資やデータ分断などが起こりやすくなります。

ウ：情報システム戦略は、ITを事業目的の達成へ結び付けるための方向性です。

エ：費用だけでなく効果・リスク・運用も含めて評価します。

総合解説：システム戦略では「何を導入するか」だけでなく、「なぜ導入し、どの経営課題を解決するか」を明確にします。

対象：2026年度 / 基準日 2026-09-05

0122 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：基礎

DX（デジタルトランスフォーメーション）の考え方として最も適切なものはどれか。

ア：紙の帳票をPDFに置き換えれば、必ずDXが完了したとみなす。

イ：既存業務を一切見直さず、端末だけ新しくすることをDXと定義する。

ウ：IT部門だけの効率化であり、事業や顧客価値とは無関係である。

エ：デジタル技術やデータを活用し、業務プロセスや製品・サービス、組織の在り方まで変革して価値向上を目指す。

答え・解説 正答：エ

ア：PDF化はデジタイゼーションの一例ですが、それだけで変革を意味しません。

イ：機器更新だけでは業務や価値提供の変革にならない場合があります。

ウ：DXは事業戦略や顧客価値と結び付けて考えます。

エ：DXは単なるデジタル化ではなく、デジタル技術を用いた事業・業務の変革を含みます。

総合解説：情報セキュリティマネジメントでも、DXに伴う新しいデータ利用やクラウド利用のリスクを、事業目的と合わせて評価する必要があります。

対象：2026年度 / 基準日 2026-09-05

0123 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：基礎

BYOD（Bring Your Own Device）の説明として最も適切なものはどれか。

ア：従業員の私物端末を、組織が定めた条件の下で業務利用する形態であり、端末管理やデータ分離などの統制が必要になる。

イ：会社支給端末以外の利用を法律で全面禁止する制度である。

ウ：個人端末であれば組織のセキュリティポリシーを適用できないため、管理は不要である。

エ：私物端末を使えば情報漏えいリスクは必ずゼロになる。

答え・解説 正答：ア

ア：BYODは私物端末の業務利用であり、利便性とともに管理・プライバシー・データ保護上の課題があります。

イ：BYODの可否は組織の方針やリスクに基づいて決めます。

ウ：私物端末でも業務データを扱う以上、必要な統制が求められます。

エ：端末紛失や不正アプリなどのリスクは残ります。

総合解説：BYODでは、利用可能端末、OS要件、認証、暗号化、業務データ領域、紛失時対応、退職時データ削除などを明確にします。

対象：2026年度 / 基準日 2026-09-05

0124 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：標準

BYODを導入する際の管理策として最も適切なものはどれか。

ア：私物なので組織は最低OSバージョンや認証要件を定めない。

イ：端末登録、画面ロック、暗号化、更新、紛失時の遠隔対応、業務データの分離など、リスクに応じた利用条件を定める。

ウ：紛失しても個人所有のため組織へ報告しなくてよい。

エ：業務データを個人用クラウドへ自由に複製してよいとする。

答え・解説 正答：イ

ア：古いOSや弱い認証は組織の情報資産へ影響します。

イ：私物端末でも業務情報を扱う以上、組織は必要なセキュリティ要件と対応手順を定めるべきです。

ウ：紛失は情報漏えい事故につながるため、報告と対応が必要です。

エ：許可されない個人サービスへの複製は情報管理を困難にします。

総合解説：BYODでは、組織のセキュリティ要求と従業員のプライバシーの双方を考慮し、管理範囲を明示することが重要です。

対象：2026年度 / 基準日 2026-09-05

0125 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：標準

従業員が公開型の生成AIサービスに顧客一覧を貼り付け、メール文案を作ろうとしている。最も適切な対応はどれか。

ア：生成AIは入力内容を必ず組織内だけで処理するので、どの情報でも自由に入力してよい。

イ：出力を削除すれば入力データの取扱条件は確認しなくてよい。

ウ：利用規程とサービスのデータ取扱条件を確認し、許可されていない機密情報・個人情報は入力しない。必要なら承認済み環境や匿名化したデータを用いる。

エ：業務効率化につながる場合は、社内規程より個人判断を優先する。

答え・解説 正答：ウ

ア：外部サービスでのデータ取扱いを一律に保証することはできません。

イ：入力時点で外部サービスへ情報を送信しているため、出力削除だけでは十分ではありません。

ウ：外部AIサービスへ入力した情報の保存・学習利用・提供条件はサービスにより異なるため、組織ルールと契約条件に従う必要があります。

エ：業務利用は組織のセキュリティ・法務・契約ルールに従います。

総合解説：生成AI活用では、入力データの機密性、出力の信頼性、知的財産、個人情報などのリスクを事前に評価し、用途別ルールを定めます。

対象：2026年度 / 基準日 2026-09-05

0126 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：標準

生成AIが作成したセキュリティ手順書案を業務で利用する際、最も適切な対応はどれか。

ア：AIが自然な文章を生成した場合は、内容を確認せず正式手順書にする。

イ：AIの回答は常に最新法令に一致するので、基準日を確認しない。

ウ：複数回同じ回答が出れば、外部根拠がなくても正しいとみなす。

エ：出力に誤りや根拠のない内容が含まれる可能性を前提に、担当者が一次情報や社内基準と照合して検証する。

答え・解説 正答：エ

ア：文章の自然さは正確性を保証しません。

イ：モデルの知識やサービス仕様によって最新性は保証されません。

ウ：同じ出力の再現は事実性の根拠にはなりません。

エ：生成AIはもっともらしい誤情報を出すことがあるため、重要な業務利用では人による検証が必要です。

総合解説：生成AIは支援ツールとして利用し、重要な判断・法令・セキュリティ設定は一次情報と責任者の確認を組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0127 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：標準

全社で生成AIを利用する際のガバナンスとして最も適切なものはどれか。

ア：許可するサービスと用途、入力禁止情報、出力確認、記録、事故報告などを定め、リスクや技術変化に応じて見直す。

イ：利用ルールは作らず、各従業員がサービス規約を個別判断する。

ウ：生成AIを導入したら情報セキュリティ教育は不要にする。

エ：一度ルールを作った後は、サービス仕様が変わっても永久に更新しない。

答え・解説 正答：ア

ア：AI利用は技術・契約・脅威が変化するため、組織的ルールと継続的見直しが必要です。

イ：個人判断に任せると情報取扱いや品質基準がばらつきます。

ウ：新しいリスクがあるため、むしろ教育・周知が重要です。

エ：環境変化に合わせて管理策を更新する必要があります。

総合解説：生成AIの利活用では、便益だけでなくリスクを評価し、役割、手続、教育、モニタリングを含むガバナンスを構築します。

対象：2026年度 / 基準日 2026-09-05

0128 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：標準

顧客対応システムの刷新案を比較する際、投資対効果を評価する方法として最も適切なものはどれか。

ア：初期購入価格だけで決め、運用費や移行費は無視する。

イ：導入・運用コストだけでなく、処理時間短縮、売上機会、品質向上、リスク低減など期待効果を定量・定性の両面で評価する。

ウ：効果は測定せず、最新技術を使っている案を自動的に採用する。

エ：現行業務の課題を確認せず、全ての処理を同じ方法で自動化する。

答え・解説 正答：イ

ア：初期費用以外にも保守・教育・移行などのコストが発生します。

イ：システム投資は、ライフサイクルコストと事業効果を合わせて評価することが重要です。

ウ：技術の新しさ自体は投資効果を保証しません。

エ：課題を把握せず自動化すると非効率な業務を固定化する場合があります。

総合解説：情報システム利用実態の評価や投資対効果分析を通じて、導入後も期待した価値が得られているか確認します。

対象：2026年度 / 基準日 2026-09-05

0129 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：応用

複数部門で同じデータを紙に転記して承認している業務をDXする。最も適切な進め方はどれか。

ア：現行の紙手順を一切変えず、全て画像化することだけを目的にする。

イ：業務分析をせず、各部門が別々のデータベースを新設する。

ウ：現行業務の目的と課題を分析し、不要な工程や重複を見直した上で、デジタル化・自動化による新しい業務プロセスを設計する。

エ：自動化できるかだけで判断し、内部統制やセキュリティ要件は考慮しない。

答え・解説 正答：ウ

ア：非効率な手順をそのまま電子化しても根本改善にならない場合があります。

イ：データ分断や重複入力を増やすおそれがあります。

ウ：DXでは、単に現行作業を電子化するだけでなく、業務プロセス自体の再設計を検討します。

エ：自動化後も統制・セキュリティを満たす必要があります。

総合解説：BPRやRPAなどは手段です。まず業務目的と課題を明確にし、統制を維持しつつ、より良いプロセスへ変えることが重要です。

対象：2026年度 / 基準日 2026-09-05

0130 システム戦略・企業活動 > システム戦略・DX・BYOD・生成AI活用 ｜ 難易度：応用

問い合わせ対応に生成AIを導入するPoCを計画している。最も適切な評価設計はどれか。

ア：回答速度だけを測り、誤回答や情報漏えいは評価対象外とする。

イ：PoCなら実データを制限なく入力し、事故が起きても記録しない。

ウ：AI利用の効果は主観だけで判断し、比較対象や評価基準を設けない。

エ：回答時間や担当者工数などの効果に加え、誤回答率、機密情報の取扱い、利用者への影響、ログ・監視方法などのリスク指標も設定する。

答え・解説 正答：エ

ア：速度向上だけでは品質やセキュリティを評価できません。

イ：PoCでもデータ保護や事故記録は必要です。

ウ：事前に指標を定めると客観的に比較・判断できます。

エ：AI導入は便益とリスクを両方測定し、採用可否や追加対策を判断することが重要です。

総合解説：生成AIは有効性が高い一方で固有のリスクもあります。小規模検証でも目的、データ範囲、評価指標、責任者、停止条件を明確にすると安全に検証できます。

対象：2026年度 / 基準日 2026-09-05

0131 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：基礎

PDCAサイクルの正しい順序はどれか。

ア：Plan → Do → Check → Act

イ：Plan → Check → Do → Act

ウ：Do → Plan → Act → Check

エ：Check → Act → Plan → Do

答え・解説 正答：ア

ア：PDCAは計画、実行、評価、改善を繰り返す管理サイクルです。

イ：実行前に評価を挟む順序ではありません。

ウ：計画より先に実行する並びではありません。

エ：CheckとActの後にPlanへ戻ることはありますが、基本順序の開始点をPlanとした表現ではありません。

総合解説：情報セキュリティでも、方針・計画を実施し、監視や監査で評価し、是正・改善して次の計画へ反映します。

対象：2026年度 / 基準日 2026-09-05

0132 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：基礎

情報セキュリティ教育について、PDCAのCheckに該当する活動として最も適切なものはどれか。

ア：年間教育計画と目標を決める。

イ：受講率、理解度テスト、模擬フィッシング結果などを測定し、計画した目標との差を評価する。

ウ：計画した研修を実施する。

エ：評価結果を基に教材や対象者を改善する。

答え・解説 正答：イ

ア：年間計画の策定はPlanに該当します。

イ：Checkは、実施結果を測定・評価する段階です。

ウ：研修の実施はDoです。

エ：改善策の実施・反映はActに該当します。

総合解説：PDCAは用語暗記だけでなく、具体的な管理活動をどの段階に置くか判断できることが重要です。

対象：2026年度 / 基準日 2026-09-05

0133 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：基礎

BCPとBCMの関係として最も適切なものはどれか。

ア：BCMは災害時だけ使う連絡先一覧を指し、BCPより範囲が狭い。

イ：BCPは情報システムのバックアップ製品名である。

ウ：BCPは事業継続のための具体的な計画であり、BCMはその計画の策定・訓練・評価・改善などを継続的に管理する考え方である。

エ：BCPとBCMはいずれも財務諸表の種類である。

答え・解説 正答：ウ

ア：BCMは平常時の分析、訓練、改善も含むため、災害時連絡だけではありません。

イ：BCPは製品名ではなく事業継続計画です。

ウ：BCPは計画、BCMは事業継続を継続的に管理する枠組みとして整理できます。

エ：財務諸表とは無関係です。

総合解説：BCMでは、BIAやリスク評価に基づいてBCPを作り、訓練・レビュー・改善を継続します。

対象：2026年度 / 基準日 2026-09-05

0134 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：標準

BIA（Business Impact Analysis）の主な目的として最も適切なものはどれか。

ア：全社員の給与額を比較して重要業務を決める。

イ：システムの脆弱性スキャンだけを実施する。

ウ：災害発生後に原因究明だけを行う。

エ：業務停止による影響を時間経過も含めて分析し、重要業務や復旧優先度、必要な復旧目標を決める材料にする。

答え・解説 正答：エ

ア：個人の給与額は業務重要度の評価基準そのものではありません。

イ：脆弱性スキャンは技術的なセキュリティ評価で、BIAとは目的が異なります。

ウ：BIAは平常時に事前実施し、復旧優先度を決めます。

エ：BIAは、業務が止まった場合の事業影響を分析し、継続戦略の基礎にします。

総合解説：売上損失、顧客影響、法令・契約違反、安全への影響などを評価し、どの業務をどの程度の時間で復旧させるかを検討します。

対象：2026年度 / 基準日 2026-09-05

0135 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：標準

決済業務は停止2時間で顧客影響が重大になる一方、社内研修予約は停止3日でも影響が小さい。BIAの結果として最も適切な判断はどれか。

ア：決済業務を高い復旧優先度とし、より短い目標時間を設定する方向で検討する。

イ：両業務を必ず同じ時間で復旧する。

ウ：影響が小さい社内研修予約を先に復旧する。

エ：業務影響を見ず、システムのサーバ台数だけで優先度を決める。

答え・解説 正答：ア

ア：BIAは業務停止の影響と許容時間を踏まえ、復旧優先度を定めるために使います。

イ：業務ごとに重要度と許容停止時間は異なります。

ウ：重大影響が早く生じる業務を後回しにするのは不合理です。

エ：サーバ台数は業務影響の代理指標にはなりません。

総合解説：技術的な復旧しやすさだけでなく、事業への影響を基準に優先順位を決める点がBIAの重要ポイントです。

対象：2026年度 / 基準日 2026-09-05

0136 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：標準

BIAで「受注受付は4時間を超える停止が許容できない」と判明した。次の対応として最も適切なものはどれか。

ア：BIAを保存するだけで、具体的な対策には反映しない。

イ：必要な復旧目標を満たすため、代替手段、要員、システム冗長化、バックアップ、連絡手順などの継続戦略を検討する。

ウ：停止時間の要求を無視し、最も安価な復旧方式だけを選ぶ。

エ：平常時の担当者一人だけが手順を知っていれば十分とする。

答え・解説 正答：イ

ア：分析結果が計画へつながらなければ事業継続能力は高まりません。

イ：BIAは分析で終わらせず、その結果を継続戦略とBCPへ反映します。

ウ：復旧目標を満たさない方式では事業要件を達成できません。

エ：属人化すると担当者不在時に計画が機能しないおそれがあります。

総合解説：復旧目標に応じて、技術対策と業務代替策を組み合わせます。コストとのバランスも必要ですが、BIAで示した重要度を基準に判断します。

対象：2026年度 / 基準日 2026-09-05

0137 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：標準

BCP訓練を定期的に実施する目的として最も適切なものはどれか。

ア：訓練を一度実施すれば、その後の組織変更やシステム変更は考慮しなくてよい。

イ：訓練では成功したことだけを記録し、問題は残さない。

ウ：手順が実際に機能するか、連絡先や役割が最新か、想定した時間内に行動できるかを確認し、改善点を見つける。

エ：本番障害が起きるまで手順を試さない方が安全である。

答え・解説 正答：ウ

ア：環境変化により計画は陳腐化するため、継続的な確認が必要です。

イ：問題点こそ改善に重要な情報です。

ウ：訓練は計画の実効性を検証し、課題を改善するために行います。

エ：未検証の手順は緊急時に機能しない可能性があります。

総合解説：BCMでは、訓練・評価・改善を継続することで、BCPを「作っただけ」の文書にしないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0138 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：標準

重要業務が外部クラウドと決済代行会社に依存している。BIA・BCMで最も適切な対応はどれか。

ア：自社設備ではないため外部依存はBIA対象外とする。

イ：委託契約があれば外部サービスは絶対に停止しないとみなす。

ウ：外部事業者の停止時は顧客影響が生じても何も準備しない。

エ：外部サービス停止が業務へ与える影響も分析し、代替手段、連絡、契約上の復旧条件などを継続計画に反映する。

答え・解説 正答：エ

ア：自社管理外であっても業務影響は自社に及ぶため分析が必要です。

イ：契約は停止可能性そのものをゼロにはしません。

ウ：代替策や連絡経路を準備することで影響を抑えられます。

エ：重要業務の依存関係には外部供給者も含まれます。

総合解説：BIAでは業務、システム、要員、施設、外部サービスなどの依存関係を把握し、単一の前提に依存しない継続戦略を検討します。

対象：2026年度 / 基準日 2026-09-05

0139 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：応用

地震時にBCPを発動したところ、連絡網の一部が古く、代替拠点への切替に予定より時間がかかった。復旧後の対応として最も適切なものはどれか。

ア：実績と計画の差を振り返り、原因を分析して連絡網・手順・訓練内容を更新し、次回のBCMへ反映する。

イ：復旧できたので問題点は記録せず、同じBCPをそのまま使い続ける。

ウ：担当者個人の注意不足だけとして処理し、手順や体制は見直さない。

エ：BCPの文書を削除し、次回は即興で対応する。

答え・解説 正答：ア

ア：実際の対応で得た課題を継続的改善へ結び付けることがBCMの重要な活動です。

イ：同じ問題を再発させないため、差異を記録し改善すべきです。

ウ：個人要因だけでなく仕組み・訓練・連絡先管理を見直します。

エ：即興対応に依存すると組織的な再現性がありません。

総合解説：事業継続は一度完成するものではありません。組織・技術・委託先の変化や訓練・実災害の結果に応じて更新します。

対象：2026年度 / 基準日 2026-09-05

0140 システム戦略・企業活動 > 経営管理・PDCA・BCM・BIA ｜ 難易度：応用

全社BCMを情報システム部門だけの課題として進めている。最も適切な評価はどれか。

ア：BCMはサーバ復旧だけを扱うので、IT部門だけで十分である。

イ：事業継続は業務優先順位、顧客対応、要員、施設、資金、外部関係者を含むため、経営層と各業務部門が関与して方針と優先順位を決める必要がある。

ウ：業務部門は復旧優先順位を知らなくても、システム部門が全て決めればよい。

エ：経営層は災害発生後に初めて参加すればよく、平常時の方針決定は不要である。

答え・解説 正答：イ

ア：IT復旧は重要ですが、要員・施設・顧客・資金など非IT要素もあります。

イ：BCMは事業全体の継続を対象とするため、経営と業務の意思決定が不可欠です。

ウ：復旧優先順位は業務影響を理解する部門との合意が必要です。

エ：平常時に方針・責任・優先順位を決めておく必要があります。

総合解説：情報システムの災害復旧はBCMの一部です。全社の重要業務を継続するには、経営層のガバナンスと横断的な連携が必要です。

対象：2026年度 / 基準日 2026-09-05

0141 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：基礎

固定費の例として最も適切なものはどれか。

ア：販売数量に比例して増える商品の仕入原価。

イ：利用件数に比例して課金されるAPI使用料。

ウ：生産量が短期的に増減しても一定額が発生する事務所の月額賃借料。

エ：製品1個当たり一定額かかる梱包材費。

答え・解説 正答：ウ

ア：仕入原価は販売・生産量に応じて増減する代表的な変動費です。

イ：従量課金は利用量に応じて変わるため変動費として扱いやすい費用です。

ウ：固定費は、一定の範囲・期間では活動量に直接比例せず発生する費用です。

エ：個数に比例する梱包材費も変動費です。

総合解説：損益分岐点分析では、固定費と変動費を区別することが基本です。実務では完全に固定・変動に分けにくい費用もあります。

対象：2026年度 / 基準日 2026-09-05

0142 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：基礎

粗利益（売上総利益）の基本的な考え方として最も適切なものはどれか。

ア：売上高から法人税だけを差し引いた利益である。

イ：現金残高から借入金を差し引いた金額である。

ウ：売上高から固定資産の帳簿価額だけを差し引いた利益である。

エ：売上高から売上原価を差し引いた利益である。

答え・解説 正答：エ

ア：法人税だけを引く定義ではありません。

イ：現金と借入金の差は粗利益を表しません。

ウ：固定資産帳簿価額だけを控除する定義ではありません。

エ：粗利益は、売上高と売上原価の差額です。

総合解説：会計の基礎では、売上高、売上原価、粗利益、営業利益などの関係を把握し、IT投資の事業影響を理解する材料にします。

対象：2026年度 / 基準日 2026-09-05

0143 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：基礎

損益分岐点売上高の説明として最も適切なものはどれか。

ア：売上高と総費用が等しくなり、利益が0となる売上高である。

イ：売上高が常に最大となる売上高である。

ウ：固定費が0になる売上高である。

エ：現金預金が借入金と等しくなる売上高である。

答え・解説 正答：ア

ア：損益分岐点では、売上による収益と固定費・変動費を含む総費用が等しくなります。

イ：最大売上を示す指標ではありません。

ウ：固定費自体が0になることを意味しません。

エ：貸借対照表の残高比較を表す概念ではありません。

総合解説：損益分岐点分析は、売上規模と費用構造から利益が出始める水準を把握するために使います。

対象：2026年度 / 基準日 2026-09-05

0144 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：標準

固定費が600万円、変動費率が60%の事業がある。損益分岐点売上高として最も適切なものはどれか。

ア：変動費率60%をそのまま分母に使い、600万円÷0.6＝1,000万円と求める。

イ：限界利益率を1−60%＝40%とし、600万円÷0.4＝1,500万円と求める。

ウ：固定費600万円をそのまま損益分岐点売上高とみなし、600万円とする。

エ：限界利益率を根拠なく25%と置き、600万円÷0.25＝2,400万円と求める。

答え・解説 正答：イ

ア：分母には変動費率ではなく、1−変動費率で求める限界利益率を使います。

イ：変動費率60%なら限界利益率は40%です。損益分岐点売上高＝固定費÷限界利益率＝600÷0.4＝1,500万円です。

ウ：固定費だけでは損益分岐点売上高は決まりません。

エ：提示条件から限界利益率を25%とする根拠はありません。

総合解説：損益分岐点売上高は「固定費 ÷ (1−変動費率)」で求められます。単位と率の扱いを確認して計算します。

対象：2026年度 / 基準日 2026-09-05

0145 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：標準

減価償却の説明として最も適切なものはどれか。

ア：固定資産を購入したら必ずその日の現金支出額と同額を毎年費用計上する。

イ：借入金の元本返済額を利益計算上の費用として均等配分する。

ウ：長期間使用する固定資産の取得原価を、その使用期間などにわたって費用配分する考え方である。

エ：売上高の一定割合を将来の税金として積み立てる手続である。

答え・解説 正答：ウ

ア：毎年同額になる方法もありますが、購入日の現金支出額そのものを毎年費用にするわけではありません。

イ：借入金元本の返済と減価償却は別の概念です。

ウ：減価償却は、固定資産の取得原価を利用期間に配分して費用化する会計処理です。

エ：税金の積立手続ではありません。

総合解説：IT設備やソフトウェア投資のコストを理解する際、現金支出と会計上の費用計上時期が一致しない場合がある点に注意します。

対象：2026年度 / 基準日 2026-09-05

0146 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：標準

ある時点の資産、負債、純資産の状態を把握するために主に用いる財務諸表はどれか。

ア：キャッシュフロー計算書だけ。

イ：WBS。

ウ：RFP。

エ：貸借対照表。

答え・解説 正答：エ

ア：キャッシュフロー計算書は一定期間の現金及び現金同等物の流れを示す資料です。

イ：WBSはプロジェクト作業を分解する管理資料です。

ウ：RFPはベンダーへ提案を依頼する文書です。

エ：貸借対照表は、一定時点の財政状態を資産・負債・純資産で示します。

総合解説：財務諸表は目的が異なります。貸借対照表は時点の財政状態、キャッシュフロー計算書は期間中の資金の流れを把握するのに使います。

対象：2026年度 / 基準日 2026-09-05

0147 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：標準

流動資産が1,200万円、流動負債が800万円である。流動比率として最も適切なものはどれか。

ア：150%。流動資産 ÷ 流動負債 × 100 で求める。

イ：66.7%。流動負債 ÷ 流動資産 × 100 で求める。

ウ：400万円。流動資産から流動負債を引く。

エ：2,000万円。流動資産と流動負債を合計する。

答え・解説 正答：ア

ア：流動比率＝流動資産÷流動負債×100なので、1,200÷800×100＝150%です。

イ：分子と分母が逆で、流動比率の式ではありません。

ウ：差額は運転資本の一つの見方ですが、流動比率ではありません。

エ：単純合計は流動比率を表しません。

総合解説：流動比率は短期的な支払能力を見る代表的な指標の一つです。単独で企業の安全性を断定せず、他の情報と合わせて評価します。

対象：2026年度 / 基準日 2026-09-05

0148 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：標準

複数の意思決定と、その後に起こり得る結果を枝分かれで整理して比較したい。適した手法はどれか。

ア：パレート図。

イ：デシジョンツリー。

ウ：WBS。

エ：DNS。

答え・解説 正答：イ

ア：パレート図は項目を大きい順に並べ、重点管理対象を見つけるのに使う品質管理手法です。

イ：デシジョンツリーは意思決定と結果の分岐を木構造で表し、選択肢を整理するのに使えます。

ウ：WBSはプロジェクト作業の分解に使います。

エ：DNSはネットワークの名前解決を行う仕組みです。

総合解説：業務分析では、目的に応じてシミュレーション、デシジョンツリー、QC手法などを使い分けます。

対象：2026年度 / 基準日 2026-09-05

0149 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：応用

ヘルプデスクの問い合わせ理由を集計したところ、少数の原因が全件数の大半を占めている。重点的に改善する原因を把握するため最も適切な手法はどれか。

ア：IPアドレスの一覧表を作る。

イ：貸借対照表だけを比較する。

ウ：原因別件数を多い順に並べ、累積比率も確認できるパレート図を用いる。

エ：暗号鍵の長さを延ばす。

答え・解説 正答：ウ

ア：IPアドレス一覧は問い合わせ原因の重点分析には適しません。

イ：貸借対照表は財政状態を示す財務諸表で、原因別件数分析の手法ではありません。

ウ：パレート図は、件数や損失などを大きい順に並べ、重点的に対処すべき項目を把握するのに適します。

エ：暗号鍵長の変更は問い合わせ原因の可視化手法ではありません。

総合解説：業務改善では、データを分類・可視化し、影響の大きい原因から対策することで限られた資源を有効に使えます。

対象：2026年度 / 基準日 2026-09-05

0150 システム戦略・企業活動 > 業務分析・会計／コストの基礎 ｜ 難易度：応用

オンプレミス案とクラウド案を比較している。初期費用だけではなく経済性を適切に比較する方法はどれか。

ア：初期購入価格だけを比較し、運用費はどちらも0円と仮定する。

イ：金額が不明な項目は全て無視し、最も宣伝が多い案を選ぶ。

ウ：セキュリティ事故や停止による事業影響はコスト評価と無関係として必ず除外する。

エ：導入費、利用料、保守、運用要員、回線、移行、教育、更新・終了時の費用など、利用期間全体で発生するコストを同じ前提で比較する。

答え・解説 正答：エ

ア：初期費用が安くても、継続費用が高ければ総費用は逆転します。

イ：不確実な費用も前提を置いて感度分析するなど、判断材料に含めるべきです。

ウ：リスクによる損失や対策費も、意思決定上重要な経済的要素になり得ます。

エ：システム案の経済性は初期費用だけでなく、運用・変更・終了まで含むライフサイクル全体のコストで比較します。

総合解説：会計・コストの基礎は、単なる計算問題ではなく、IT投資を事業として比較評価するために使います。前提条件を揃え、見えにくい運用・移行コストも含めます。

対象：2026年度 / 基準日 2026-09-05