問題 0001 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：基礎

データベースの説明として、最も適切なものはどれか。

ア. 関連するデータを体系的に整理し、利用しやすい形で蓄積したもの。

イ. 処理手順だけを記述したプログラム。

ウ. ネットワーク機器の接続だけを示す図。

エ. 紙の文書を画像化する装置。

解答・解説 正答：ア

ア：データベースは業務で扱うデータを体系的に整理し、検索や更新を行いやすくしたデータの集合です。

イ：プログラムは処理手順を記述するもので、データベースとは異なります。

ウ：ネットワーク構成図の説明に近く、データの集合ではありません。

エ：スキャナなどの入力装置の説明です。

総合解説：データベースでは、関連データを構造的に管理し、効率的に取り出したり更新したりできることが重要です。

問題 0002 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：基礎

データを構造的に蓄積し、一貫性を保ちながら検索・更新などを管理するソフトウェアはどれか。

ア. OSだけ

イ. DBMS

ウ. Webブラウザ

エ. コンパイラ

解答・解説 正答：イ

ア：OSはコンピュータ資源を管理する基本ソフトウェアで、データベース管理に特化したものではありません。

イ：DBMSはDatabase Management Systemで、データベースの作成・検索・更新・保全などを管理します。

ウ：Webページを閲覧するソフトウェアです。

エ：プログラム言語を翻訳するソフトウェアです。

総合解説：DBMSは複数利用者によるデータ利用を支え、検索、更新、整合性維持、障害回復などを担います。

問題 0003 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：標準

データを表形式で管理し、表同士の関係を利用して扱うDBMSはどれか。

ア. KVS

イ. グラフ指向データベース

ウ. RDBMS

エ. ファイル圧縮ソフト

解答・解説

正答：ウ

ア：キーと値の組でデータを管理するNoSQLの一種です。

イ：ノードとエッジの関係を中心に扱うデータベースです。

ウ：RDBMSは関係データベース管理システムで、表形式のデータと表間の関係を扱います。

エ：データ量を減らすソフトウェアで、DBMSではありません。

総合解説：ITパスポートではRDBMSに加えて、KVS、ドキュメント指向、グラフ指向などNoSQLの基本的な種類も押さえます。

問題 0004 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：標準

一意なキーと、それに対応する値の組でデータを管理する方式はどれか。

ア. RDBMSだけ

イ. E-R図

ウ. 正規化

エ. KVS

解答・解説

正答：エ

ア：表形式の関係データベースを管理します。

イ：データと関連を図で表す設計手法です。

ウ：データの重複や更新時の不整合を減らすための設計上の考え方です。

エ：KVSはKey-Value Storeで、キーと値の組でデータを管理します。

総合解説：KVSはNoSQLの代表例で、単純なキーによる高速な参照などに利用されます。

問題 0005 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：標準

JSONのような文書単位でデータを格納し、項目構造が柔軟なデータを扱いやすいNoSQLはどれか。

ア. ドキュメント指向データベース

イ. グラフ指向データベース

ウ. KVS

エ. CSVファイル

解答・解説

正答：ア

ア：文書単位で構造化データを管理するNoSQLです。

イ：要素間のつながりを中心に表現するDBです。

ウ：キーと値の組で管理する方式です。

エ：区切り文字で表形式データを表すファイル形式です。

総合解説：NoSQLには用途に応じてKVS、ドキュメント指向、グラフ指向などがあります。

問題 0006 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：標準

SNSで利用者同士の友人関係やフォロー関係を中心に検索したい。適したデータベースの考え方はどれか。

ア. KVSだけ

イ. グラフ指向データベース

ウ. 表計算ソフト

エ. 画像ファイル

解答・解説

正答：イ

ア：キーと値の単純な参照には向きますが、複雑な関係の探索を主目的とする方式ではありません。

イ：人物や物をノード、関係をエッジとして扱うため、つながりの分析に向きます。

ウ：小規模な表データ管理には使えますが、関係探索を目的とするDBMSではありません。

エ：データベース方式ではありません。

総合解説：データモデルは、管理したいデータの構造や利用方法に応じて選ぶことが重要です。

問題 0007 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：応用

各部署が同じ顧客情報を別々のファイルで管理し、内容の食い違いが増えている。改善策として最も適切なものはどれか。

ア. 部署ごとにさらに複製ファイルを増やす。

イ. 更新履歴を残さず自由に書き換える。

ウ. DBMSで共通のデータを一元的に管理し、更新ルールやアクセス権を整える。

エ. 顧客情報を画像として保存するだけにする。

解答・解説 正答：ウ

ア：重複や不整合が増える可能性があります。

イ：整合性や追跡性が低下します。

ウ：共通データをDBMSで管理することで、重複管理や不整合を減らしやすくなります。

エ：検索や更新の効率化にはつながりにくいです。

総合解説：DBMSはデータを共有・一元管理し、一貫性や検索性を高めるために利用されます。

問題 0008 [6-1 データベース] > [DB・DBMS・データモデル] ｜ 難易度：応用

商品マスタのような定型項目の表データと、SNSの複雑なつながりデータを扱う。考え方として最も適切なものはどれか。

ア. どのデータでも必ずKVSだけを使う。

イ. 表形式データは必ず画像として保存する。

ウ. DBMSの種類を確認せず、名称だけで選ぶ。

エ. データの構造や利用目的に応じて、RDBMSやグラフ指向DBなど適した方式を選ぶ。

解答・解説 正答：エ

ア：用途により他方式が適する場合があります。

イ：構造化データとして扱いにくくなります。

ウ：要件との適合性を判断できません。

エ：一つの方式が全用途に最適とは限らず、データ構造と利用方法に応じた選択が必要です。

総合解説：DB方式は、データの構造、検索方法、更新方法などを基に選定します。

問題 0009 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：基礎

データベース設計で、実体と実体間の関連を図で整理するものはどれか。

ア. E-R図

イ. フローチャート

ウ. ガントチャート

エ. ネットワーク構成図

解答・解説 正答：ア

ア：E-R図はEntityとRelationshipを用いてデータとその関連を表現します。

イ：処理の流れを表す図です。

ウ：作業日程を表す図です。

エ：機器や通信経路を表す図です。

総合解説：E-R図はデータベース設計で、業務上の対象とその関係を整理するために利用します。

問題 0010 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：基礎

表の各行を一意に識別するために用いる項目はどれか。

ア. 外部キー

イ. 主キー

ウ. インデックス

エ. コメント

解答・解説 正答：イ

ア：他の表の主キーなどを参照し、表同士を関連付ける項目です。

イ：主キーは各レコードを一意に特定できる値を持つ項目です。

ウ：検索を効率化するための仕組みです。

エ：説明用の情報で、行の識別子ではありません。

総合解説：主キーは重複しない値を用いて各レコードを一意に識別します。

問題 0011 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：標準

受注表の顧客IDが顧客表の顧客IDを参照し、受注と顧客を関連付けている。この受注表の顧客IDは何か。

ア. 主キー

イ. インデックス

ウ. 外部キー

エ. トランザクション

解答・解説 正答：ウ

ア：受注表自身の各行を一意に識別する項目とは限りません。

イ：検索高速化のための仕組みです。

ウ：他の表の主キーなどを参照して表同士を関連付ける項目です。

エ：一連の処理を一つの単位として扱う考え方です。

総合解説：外部キーは表同士の関係を表現するために利用されます。

問題 0012 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：標準

顧客表に「顧客ID、氏名、住所」という項目があり、顧客1人分の一行を表す用語はどれか。

ア. フィールド

イ. 主キー

ウ. テーブル名

エ. レコード

解答・解説 正答：エ

ア：顧客IDや氏名など個々の項目を指します。

イ：行を一意に識別する項目です。

ウ：表全体を識別する名称です。

エ：一つの対象に関する複数項目をまとめた一行をレコードといいます。

総合解説：表では、列に相当する項目をフィールド、行に相当する一件分のデータをレコードと呼びます。

問題 0013 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：標準

大量のデータから特定の値を検索しやすくするために用いる仕組みはどれか。

ア. インデックス

イ. 外部キー

ウ. E-R図

エ. ロールバック

解答・解説 正答：ア

ア：インデックスは検索対象の値とデータ位置の対応を持ち、検索の効率化に役立ちます。

イ：表同士の関連付けに使います。

ウ：データと関連を設計段階で表す図です。

エ：トランザクションを取り消して元の状態へ戻す処理です。

総合解説：インデックスは検索性能を高める目的で利用されますが、更新時の処理負荷なども考慮します。

問題 0014 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：応用

一つの表に同じ顧客住所を何度も記録した結果、住所変更時に一部だけ更新され不整合が生じた。改善の考え方として最も適切なものはどれか。

ア. 同じ住所をさらに多くの列へ複製する。

イ. データの重複を減らし、更新時の不整合を起こしにくくするよう表を整理する。

ウ. 更新を禁止して古い情報を残す。

エ. 主キーを削除して行を識別できなくする。

解答・解説 正答：イ

ア：重複が増え不整合の原因になります。

イ：正規化は重複や更新時の不整合を減らすために行います。

ウ：最新情報を管理できません。

エ：データ管理が難しくなります。

総合解説：ITパスポートでは正規化の詳細手順より、重複や更新時の不整合を抑える必要性を理解することが重視されます。

問題 0015 [6-1 データベース] > [E-R図・主キー・外部キー・正規化の必要性] ｜ 難易度：応用

顧客表と受注表を設計する。顧客表では顧客IDで顧客を一意に識別し、受注表から顧客を参照したい。最も適切な設計はどれか。

ア. 顧客表から顧客IDを削除する。

イ. 受注表へ顧客情報を毎回全項目重複保存する。

ウ. 顧客表の顧客IDを主キーとし、受注表に顧客IDを外部キーとして持たせる。

エ. E-R図を使わず表同士の関係を考えない。

解答・解説 正答：ウ

ア：顧客を一意に識別しにくくなります。

イ：重複や不整合が増えやすくなります。

ウ：主キーで顧客を一意に識別し、外部キーで受注との関係を表現できます。

エ：設計上の関係を整理しにくくなります。

総合解説：主キー、外部キー、E-R図、正規化の必要性を組み合わせてデータ設計を考えます。

問題 0016 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：基礎

関係データベースで、条件に合う行だけを取り出す操作はどれか。

ア. 射影

イ. 結合

ウ. 挿入

エ. 選択

解答・解説 正答：エ

ア：必要な列だけを取り出す操作です。

イ：複数の表を関連付けて組み合わせる操作です。

ウ：新しい行を追加する操作です。

エ：選択は条件を指定して必要な行を抽出する操作です。

総合解説：ITパスポートではSQL文法ではなく、選択・射影・結合などの操作の意味を理解します。

問題 0017 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：基礎

関係データベースで、表から必要な列だけを取り出す操作はどれか。

ア. 射影

イ. 選択

ウ. 結合

エ. 更新

解答・解説 正答：ア

ア：射影は必要な列を選んで取り出す操作です。

イ：条件に合う行を取り出します。

ウ：複数表を組み合わせます。

エ：既存データを書き換えます。

総合解説：選択は行、射影は列を取り出す操作として区別します。

問題 0018 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：標準

顧客表と受注表を顧客IDで関連付け、顧客名と受注金額を一緒に表示する操作はどれか。

ア. 選択

イ. 結合

ウ. 射影

エ. 削除

解答・解説 正答：イ

ア：一つの表から条件に合う行を抽出する操作です。

イ：共通項目などを使って複数の表を関連付けて組み合わせます。

ウ：必要な列だけを取り出す操作です。

エ：データを取り除く操作で、表を組み合わせるものではありません。

総合解説：結合により、複数の表に分けて管理したデータを関連付けて利用できます。

問題 0019 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：標準

顧客表に新しい顧客のレコードを追加する操作はどれか。

ア. 更新

イ. 選択

ウ. 挿入

エ. 射影

解答・解説 正答：ウ

ア：既存データの値を書き換えます。

イ：条件に合う行を取り出します。

ウ：新しいデータ行を追加する操作です。

エ：必要な列を取り出します。

総合解説：挿入は新規データの追加、更新は既存データの変更です。

問題 0020 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：標準

既存顧客の住所が変わったため、顧客表の住所を新しい内容に書き換える操作はどれか。

ア. 挿入

イ. 選択

ウ. 結合

エ. 更新

解答・解説 正答：エ

ア：新しい行を追加します。

イ：条件に合う行を取り出します。

ウ：複数表を組み合わせます。

エ：既に存在するデータの内容を書き換える操作です。

総合解説：データ操作では、追加と変更を区別して適切な操作を行います。

問題 0021 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：標準

社員表から「営業部の社員」だけを対象にし、その「氏名とメールアドレス」だけを表示したい。考え方として最も適切なものはどれか。

ア. 営業部という条件で選択し、氏名とメールアドレスを射影する。

イ. 氏名だけで結合し、全列を表示する。

ウ. 新規社員を挿入してから全行削除する。

エ. 住所列だけを更新する。

解答・解説 正答：ア

ア：行を絞る選択と、列を絞る射影を組み合わせています。

イ：必要な操作と一致しません。

ウ：抽出目的とは関係ありません。

エ：検索・表示の目的とは異なります。

総合解説：関係データベースでは、選択・射影・結合などを組み合わせて必要な情報を取り出します。

問題 0022 [6-1 データベース] > [選択・射影・結合・挿入・更新] ｜ 難易度：応用

ITパスポートのデータ操作学習として最も適切なものはどれか。

ア. 複雑なSQL最適化手法だけを暗記する。

イ. SQL文の細かな文法暗記より、挿入・更新・選択・射影・結合が何をする操作かを理解する。

ウ. DB操作は一切出題範囲でないと考える。

エ. 選択と射影は同じ操作だと覚える。

解答・解説 正答：イ

ア：ITパスポートの学習深度を超えます。

イ：シラバスではSQL文法自体は問わないとされ、代表的なデータ操作の意味理解が重視されます。

ウ：代表的なデータ操作は出題範囲です。

エ：行と列を対象とする異なる操作です。

総合解説：データ操作では概念と用途を正確に区別することが重要です。

問題 0023 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：基礎

データベースで、複数の処理を一つのまとまりとして扱う単位を何というか。

ア. レコード

イ. インデックス

ウ. トランザクション

エ. 外部キー

解答・解説 正答：ウ

ア：表の一行分のデータです。

イ：検索を効率化する仕組みです。

ウ：一連のデータ操作を一つの論理的な処理単位として扱います。

エ：表同士を関連付ける項目です。

総合解説：例えば振込処理では、引落しと入金を一つのトランザクションとして扱うことで整合性を保ちます。

問題 0024 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：基礎

複数利用者が同じデータを同時更新するときの不整合を防ぐために必要な制御はどれか。

ア. 画像圧縮

イ. DNS

ウ. ロードバランシング

エ. 排他制御

解答・解説 正答：エ

ア：データ量を減らす処理です。

イ：名前とIPアドレスを対応付ける仕組みです。

ウ：処理負荷を複数装置へ分散する仕組みです。

エ：同時更新による競合を避け、データの整合性を保つために利用します。

総合解説：排他制御は複数利用者が同時にDBへアクセスする環境で重要です。

問題 0025 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：標準

二つのトランザクションが互いに相手の解放を待ち続け、どちらも処理を進められない状態はどれか。

ア. デッドロック

イ. ロールバック

ウ. コミット

エ. レプリケーション

解答・解説

正答：ア

ア：互いに必要な資源の解放を待ち合って処理が停止する状態です。

イ：処理を取り消して元の状態へ戻すことです。

ウ：トランザクションの結果を確定することです。

エ：データを複製する仕組みです。

総合解説：デッドロックは排他制御に伴って発生する可能性があるため、検出や回避が必要です。

問題 0026 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：標準

トランザクションの処理が正常終了し、その更新内容をデータベースへ確定する操作はどれか。

ア. ロールバック

イ. コミット

ウ. 選択

エ. 射影

解答・解説

正答：イ

ア：更新を取り消して元の状態へ戻します。

イ：コミットによりトランザクションの結果を確定します。

ウ：条件に合う行を抽出します。

エ：必要な列を取り出します。

総合解説：トランザクションでは、正常時にコミットし、異常時には必要に応じてロールバックします。

問題 0027 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：標準

振込処理の途中でエラーが発生したため、途中までの更新を取り消して処理前の状態へ戻す操作はどれか。

ア. コミット

イ. 結合

ウ. ロールバック

エ. 挿入

解答・解説 正答：ウ

ア：更新内容を確定する操作です。

イ：複数表を組み合わせる操作です。

ウ：途中の更新を取り消してトランザクション開始前などの状態へ戻します。

エ：新しい行を追加する操作です。

総合解説：ロールバックは処理途中の障害による不整合を防ぐために重要です。

問題 0028 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：標準

トランザクション処理で、処理を一まとまりとして確実に扱い、データの整合性を保つための代表的な性質をまとめたものはどれか。

ア. OSI参照モデル

イ. LATCH

ウ. CIA

エ. ACID特性

解答・解説 正答：エ

ア：通信機能を7層に分けるネットワークモデルです。

イ：情報整理の原則です。

ウ：情報セキュリティの機密性・完全性・可用性を表す考え方です。

エ：ACIDはトランザクションの信頼性を支える代表的な特性の総称です。

総合解説：ITパスポートではACIDの詳細な理論より、トランザクションの整合性や信頼性を支える考え方として理解します。

問題 0029 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：応用

データベース更新中にサーバ障害が発生した。復旧時に重視すべき考え方として最も適切なものはどれか。

ア. ログやバックアップなどを利用し、整合性のある状態へデータベースを回復する。

イ. 障害前後の状態を確認せず、すべてのデータを削除する。

ウ. 一部だけ更新された状態をそのまま確定する。

エ. 障害記録を残さない。

解答・解説 正答：ア

ア：障害回復では更新記録やバックアップなどを利用して、一貫した状態へ戻す必要があります。

イ：必要なデータまで失います。

ウ：整合性が崩れる可能性があります。

エ：原因分析や適切な回復が難しくなります。

総合解説：DBMSのリカバリ機能は、障害時にもデータを保全し、整合性のある状態へ回復するために利用されます。

問題 0030 [6-1 データベース] > [トランザクション・排他制御・障害回復] ｜ 難易度：応用

オンライン予約システムで同じ席を複数人が同時予約できないようにし、処理途中の障害時には中途半端な更新を残したくない。必要な考え方の組合せはどれか。

ア. 画像圧縮と動画再生

イ. 排他制御とトランザクションの障害回復

ウ. DNSとURL

エ. CSSとHTML

解答・解説 正答：イ

ア：DBの整合性管理とは関係ありません。

イ：同時更新競合には排他制御、途中障害への対処にはコミットやロールバックなどのトランザクション管理が必要です。

ウ：ネットワーク上の名前解決や資源指定に関する用語です。

エ：Web画面の構造や見た目に関する技術です。

総合解説：複数利用者が同時利用するDBでは、同時実行制御と障害回復を組み合わせてデータを保全します。

問題 0031 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：基礎

オフィスや学校など、比較的限られた範囲で構築されるネットワークはどれか。

ア. WAN

イ. VPN

ウ. LAN

エ. DNS

解答・解説 正答：ウ

ア：離れた地域のネットワーク同士を結ぶ広域ネットワークです。

イ：公衆網などを利用して仮想的な専用網を実現する仕組みです。

ウ：LANはLocal Area Networkで、建物内や敷地内など比較的狭い範囲で利用されます。

エ：ドメイン名とIPアドレスを対応付ける仕組みです。

総合解説：職場のネットワークはLANやWANなどを組み合わせて構成されます。

問題 0032 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：基礎

東京本社と大阪支社など、地理的に離れた拠点間を結ぶ広域ネットワークはどれか。

ア. LAN

イ. Bluetooth

ウ. NFC

エ. WAN

解答・解説 正答：エ

ア：比較的狭い範囲のネットワークです。

イ：近距離無線通信です。

ウ：ごく近距離の無線通信です。

エ：WANはWide Area Networkで、離れた地域のネットワークを接続します。

総合解説：WANは複数拠点のLANを通信回線などで接続する際に利用されます。

問題 0033 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：基礎

PCをネットワークへ接続するために使われるネットワークインタフェースカードの略称はどれか。

ア. NIC

イ. UPS

ウ. OCR

エ. CPU

解答・解説 正答：ア

ア：NICはNetwork Interface Cardで、端末をネットワークへ接続するためのインタフェースです。

イ：無停電電源装置です。

ウ：画像中の文字を認識する技術です。

エ：演算や制御を行うプロセッサです。

総合解説：ネットワーク接続にはNIC、ケーブル、スイッチ、ルーターなど複数の構成要素が使われます。

問題 0034 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：基礎

同一LAN内の複数機器を接続し、宛先に応じてフレームを適切なポートへ転送する装置はどれか。

ア. ルーター

イ. スイッチ

ウ. プロジェクター

エ. プリンター

解答・解説 正答：イ

ア：異なるネットワーク間のパケット転送を行う装置です。

イ：スイッチはLAN内で機器を接続し、MACアドレスなどを基に転送します。

ウ：映像を投影する装置です。

エ：紙などへ出力する装置です。

総合解説：スイッチはLAN内部の接続装置として、必要な宛先へ通信を転送します。

問題 0035 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：標準

社内LANとインターネットなど、異なるネットワーク間でパケットを転送する装置はどれか。

ア. スイッチだけ

イ. キーボード

ウ. ルーター

エ. スキャナ

解答・解説 正答：ウ

ア：主に同一LAN内の接続に利用されます。

イ：入力装置です。

ウ：ルーターは異なるネットワークを接続し、宛先IPアドレスなどを基に経路を選択します。

エ：画像入力装置です。

総合解説：ルーターはネットワーク間を接続する代表的な装置で、デフォルトゲートウェイとして使われることもあります。

問題 0036 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：標準

端末が自分のLAN外の宛先へ通信するとき、通常最初にパケットを送る相手として設定するものはどれか。

ア. DNSサーバだけ

イ. Webサーバ

ウ. メールサーバ

エ. デフォルトゲートウェイ

解答・解説 正答：エ

ア：名前解決を行うサーバで、ネットワーク外への出口そのものではありません。

イ：Webコンテンツを提供するサーバです。

ウ：電子メールを扱うサーバです。

エ：自ネットワーク外の宛先へ通信する際の出口となるルーターなどを指定します。

総合解説：デフォルトゲートウェイは、端末から別ネットワークへ通信するときの代表的な経路先です。

問題 0037 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：標準

LAN内でネットワークインタフェースを識別するために利用される代表的なアドレスはどれか。

ア. MACアドレス

イ. URL

ウ. ドメイン名

エ. ポート番号

解答・解説 正答：ア

ア：MACアドレスはネットワークインタフェースを識別するために使われます。

イ：Web資源の場所を表します。

ウ：インターネット上の名前として利用されます。

エ：同一端末内の通信先アプリケーション識別などに使われます。

総合解説：IPアドレスとMACアドレスは役割が異なり、通信の各段階で使い分けられます。

問題 0038 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：標準

一台の物理スイッチにつながる端末を、部門ごとに論理的な別LANとして分けたい。利用する技術はどれか。

ア. VPN

イ. VLAN

ウ. DNS

エ. MIMO

解答・解説 正答：イ

ア：離れた拠点や端末間で仮想的な専用通信路を作る仕組みです。

イ：VLANは物理構成とは別に論理的なLANを分割する技術です。

ウ：名前解決の仕組みです。

エ：複数アンテナを利用する無線通信技術です。

総合解説：VLANを使うと、一つの物理ネットワーク上で論理的にネットワークを分離できます。

問題 0039 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：標準

利用者の代わりにWebサーバへアクセスし、通信を中継する仕組みはどれか。

ア. ルーターだけ

イ. アクセスポイント

ウ. プロキシ

エ. NTP

解答・解説 正答：ウ

ア：ネットワーク間のパケット転送が主な役割です。

イ：無線端末をLANへ接続する装置です。

ウ：プロキシはクライアントに代わって外部サーバへアクセスし、通信を中継します。

エ：時刻同期のためのプロトコルです。

総合解説：プロキシは通信の中継、アクセス制御、キャッシュなどの目的で利用されます。

問題 0040 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：標準

Wi-Fiを利用する端末を有線LANなどへ接続するための装置はどれか。

ア. スキャナ

イ. DBMS

ウ. UPS

エ. アクセスポイント

解答・解説 正答：エ

ア：画像入力装置です。

イ：データベース管理ソフトです。

ウ：停電時の電力供給装置です。

エ：無線端末とLANを接続する無線LANの基地局のような役割を持ちます。

総合解説：無線LANではアクセスポイント、ESSID、Wi-Fi規格などの基本用語を理解します。

問題 0041 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：応用

広いオフィスで複数の無線機器を連携させ、電波が届きにくい場所を減らしながらWi-Fiエリアを広げたい。適した考え方はどれか。

ア. メッシュWi-Fi

イ. NFC

ウ. USB

エ. SMTP

解答・解説 正答：ア

ア：複数の機器が連携して無線ネットワークを構成し、カバー範囲を広げる方式です。

イ：ごく近距離の無線通信です。

ウ：有線の周辺機器接続規格です。

エ：電子メール送信などに使うプロトコルです。

総合解説：メッシュWi-Fiは複数ノードを連携させて無線LANのカバー範囲や接続性を高める方式です。

問題 0042 [6-2 ネットワーク] > [LAN・WAN・ネットワーク機器] ｜ 難易度：応用

社内の複数PCを同一LANへ接続し、そのLANをインターネットへ接続する。基本的な装置の組合せとして最も適切なものはどれか。

ア. PC間接続にプリンター、インターネット接続にスキャナを使う。

イ. PC間のLAN接続にスイッチ、異なるネットワーク間の接続にルーターを使う。

ウ. すべての通信をキーボードだけで中継する。

エ. LANとWANの違いを考えず、機器の役割も区別しない。

解答・解説 正答：イ

ア：どちらもネットワーク接続装置ではありません。

イ：スイッチは同一LAN内、ルーターは異なるネットワーク間の接続に利用します。

ウ：キーボードは入力装置です。

エ：適切なネットワーク設計になりません。

総合解説：ネットワーク構成では、LAN内接続とネットワーク間接続で機器の役割を区別します。

問題 0043 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：基礎

通信機能を7層に分けて整理したネットワークアーキテクチャはどれか。

ア. TCP/IP階層モデル

イ. E-Rモデル

ウ. OSI基本参照モデル

エ. LATCH

解答・解説 正答：ウ

ア：一般に4層で整理されるモデルです。

イ：データベース設計のモデルです。

ウ：OSI基本参照モデルはISOが策定した7層のネットワークアーキテクチャです。

エ：情報整理の原則です。

総合解説：OSI基本参照モデルでは、各層の基本的な役割と層同士の関係を理解します。

問題 0044 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：基礎

インターネットで標準的に利用される、4層から成るネットワークアーキテクチャはどれか。

ア. OSI基本参照モデル

イ. PPM

ウ. WBS

エ. TCP/IP階層モデル

解答・解説 正答：エ

ア：7層で整理する参照モデルです。

イ：事業分析手法です。

ウ：プロジェクト作業を分解する手法です。

エ：ネットワークインタフェース層、インターネット層、トランスポート層、アプリケーション層で整理します。

総合解説：TCP/IP階層モデルはインターネット通信の基本となる考え方です。

問題 0045 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：基礎

異なるコンピュータ同士が正しく通信するために必要な、データ形式や手順などの共通ルールを何というか。

ア. 通信プロトコル

イ. データベース正規化

ウ. 画像圧縮

エ. TCO

解答・解説 正答：ア

ア：通信する双方が共通の規則に従うことで、異なる環境間でも情報をやり取りできます。

イ：DB設計上の考え方です。

ウ：データ量を減らす処理です。

エ：総保有コストです。

総合解説：通信プロトコルは、送受信双方が同じ規則で通信するために必要です。

問題 0046 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：基礎

TCPとUDPの説明として、最も適切なものはどれか。

ア. TCPはWebページの記述言語である。

イ. TCPは信頼性を重視した通信、UDPは確認処理を抑えた軽量な通信で利用される。

ウ. UDPはIPアドレスをドメイン名へ変換する。

エ. TCPとUDPはどちらも画像ファイル形式である。

解答・解説 正答：イ

ア：TCPは通信プロトコルです。

イ：TCPとUDPはトランスポート層で利用され、通信制御の考え方が異なります。

ウ：それはDNSの役割です。

エ：通信プロトコルです。

総合解説：用途に応じて、信頼性や通信負荷を考えてTCPとUDPが使い分けられます。

問題 0047 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：標準

Webページの送受信に使われ、TLSによる暗号化を組み合わせたプロトコルはどれか。

ア. HTTP

イ. SMTP

ウ. HTTPS

エ. NTP

解答・解説 正答：ウ

ア：Web通信に使われますが、設問のTLSによる保護を含む表現ではありません。

イ：電子メール送信に使われるプロトコルです。

ウ：HTTPSはHTTP over TLSで、Web通信をTLSで保護します。

エ：時刻同期に使われるプロトコルです。

総合解説：Web通信ではHTTPとHTTPSの役割を区別し、HTTPSがTLSで通信を保護することを理解します。

問題 0048 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：標準

電子メールを送信する際に利用される代表的なプロトコルはどれか。

ア. POP

イ. IMAP

ウ. FTP

エ. SMTP

解答・解説 正答：エ

ア：メールサーバからメールを受信する際に利用される代表的なプロトコルです。

イ：メールをサーバ上で管理しながら利用する受信プロトコルです。

ウ：ファイル転送に使われるプロトコルです。

エ：SMTPは電子メールの送信・転送に利用されます。

総合解説：電子メールでは送信にSMTP、受信にPOPやIMAPなどが使われます。

問題 0049 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：標準

複数端末から同じメールボックスを利用し、メールをサーバ上で管理しながら閲覧する用途に適したプロトコルはどれか。

ア. IMAP

イ. POP

ウ. SMTP

エ. NTP

解答・解説

正答：ア

ア：IMAPはメールをサーバ上で管理しながら複数端末から利用しやすい方式です。

イ：メールを端末へ受信して利用する方式として代表的です。

ウ：送信に使うプロトコルです。

エ：時刻同期用プロトコルです。

総合解説：POPとIMAPはどちらもメール受信に使われますが、メールの管理方法が異なります。

問題 0050 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：標準

LANへ接続した端末へIPアドレスなどのネットワーク設定を自動的に割り当てる仕組みはどれか。

ア. DNS

イ. DHCP

ウ. FTP

エ. NTP

解答・解説

正答：イ

ア：ドメイン名とIPアドレスを対応付けます。

イ：DHCPは端末へIPアドレスなどの設定情報を自動配布します。

ウ：ファイル転送に使います。

エ：時刻を同期します。

総合解説：DHCPを利用すると、端末ごとに手作業でIP設定する負担を減らせます。

問題 0051 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：標準

複数のコンピュータの時計をネットワーク経由で同期するために利用するプロトコルはどれか。

ア. DHCP

イ. SMTP

ウ. NTP

エ. FTP

解答・解説 正答：ウ

ア：IPアドレスなどを自動設定する仕組みです。

イ：メール送信に使われます。

ウ：NTPはNetwork Time Protocolで、機器の時刻同期に使われます。

エ：ファイル転送に使われます。

総合解説：ログの時刻をそろえるなど、正確な時刻同期はシステム運用でも重要です。

問題 0052 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：標準

同じIPアドレスを持つコンピュータ上で、通信先となるアプリケーションやサービスを識別するために使われるものはどれか。

ア. MACアドレス

イ. ドメイン名

ウ. SSID

エ. ポート番号

解答・解説 正答：エ

ア：ネットワークインタフェース識別に使われます。

イ：インターネット上の名前として使われます。

ウ：無線LANのネットワーク名として使われます。

エ：ポート番号は同一端末上の通信先サービスを識別するために利用されます。

総合解説：IPアドレスが通信先端末を示し、ポート番号がその端末上のサービスを識別するイメージで理解します。

問題 0053 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：応用

IPv6が普及した主な背景の一つとして、最も適切なものはどれか。

ア. インターネット接続機器の増加に伴うIPv4アドレス不足への対応。

イ. IPv6ではIPアドレスを一切使わないため。

ウ. IPv4がWebページ記述言語だから。

エ. IPv6ではルーターが不要になるため。

解答・解説 正答：ア

ア：IPv6はIPv4より大きなアドレス空間を持ち、多数の機器へアドレスを割り当てやすくします。

イ：IPv6もIPアドレスを利用します。

ウ：IPv4はネットワーク層のプロトコルです。

エ：ネットワーク間接続にはルーターが利用されます。

総合解説：IPアドレスにはIPv4とIPv6があり、それぞれアドレス表現やアドレス空間に違いがあります。

問題 0054 [6-2 ネットワーク] > [OSI・TCP/IP・IPアドレス・通信プロトコル] ｜ 難易度：応用

Web閲覧、メール送信、ファイル転送、時刻同期に使う代表的なプロトコルの組合せとして最も適切なものはどれか。

ア. WebはNTP、メール送信はDHCP、ファイル転送はSMTP、時刻同期はFTP。

イ. WebはHTTP/HTTPS、メール送信はSMTP、ファイル転送はFTP、時刻同期はNTP。

ウ. すべてDNSだけで行う。

エ. すべてMACアドレスだけで行う。

解答・解説 正答：イ

ア：役割が入れ替わっています。

イ：それぞれシラバスに挙げられている代表的なアプリケーション層プロトコルの役割です。

ウ：DNSは名前解決の仕組みです。

エ：MACアドレスは通信サービスそのものではありません。

総合解説：代表的なプロトコルは名称だけでなく、どのサービスに使われるかを対応付けて理解します。

問題 0055 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：基礎

ドメイン名とIPアドレスを対応付ける仕組みはどれか。

ア. DHCP

イ. SMTP

ウ. DNS

エ. FTP

解答・解説 正答：ウ

ア：IPアドレスなどを端末へ自動設定する仕組みです。

イ：メール送信プロトコルです。

ウ：DNSはDomain Name Systemで、人が扱いやすいドメイン名とIPアドレスの対応を管理します。

エ：ファイル転送プロトコルです。

総合解説：インターネットではIPアドレスとドメイン名をDNSによって対応付けます。

問題 0056 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：基礎

組織内LANなどで利用し、インターネット上で直接一意に割り当てることを前提としないIPアドレスはどれか。

ア. グローバルIPアドレス

イ. MACアドレス

ウ. URL

エ. プライベートIPアドレス

解答・解説 正答：エ

ア：インターネット上で識別に使われるアドレスです。

イ：ネットワークインタフェース識別に使われます。

ウ：Web資源の場所を表します。

エ：プライベートIPアドレスは組織内などの閉じたネットワークで利用されます。

総合解説：IPv4ではグローバルIPとプライベートIPを用途に応じて使い分けます。

問題 0057 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：基礎

利用者へインターネット接続サービスを提供する事業者はどれか。

ア. ISP

イ. MVNO

ウ. DBMS

エ. CSIRT

解答・解説 正答：ア

ア：ISPはInternet Service Providerで、インターネット接続サービスを提供します。

イ：他社の移動体通信網を利用してモバイル通信サービスを提供する事業者です。

ウ：データベース管理システムです。

エ：セキュリティインシデント対応組織です。

総合解説：通信サービスではISP、回線事業者、MVNOなどの役割を区別します。

問題 0058 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：標準

自ら大規模な移動体通信網を持たず、他社の通信網を借りて携帯通信サービスを提供する事業者はどれか。

ア. ISPだけ

イ. MVNO

ウ. DNSサーバ

エ. アクセスポイント

解答・解説 正答：イ

ア：インターネット接続サービス事業者の総称で、MVNOとは役割が異なります。

イ：MVNOはMobile Virtual Network Operatorで、他社の移動体通信網を利用してサービスを提供します。

ウ：名前解決を行うサーバです。

エ：無線LAN端末をLANへ接続する装置です。

総合解説：MVNOはモバイル通信サービスの代表的な事業形態の一つです。

問題 0059 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：標準

移動中のスマートフォンが、通信を継続しながら接続先の基地局を切り替える仕組みはどれか。

ア. ローミング

イ. テザリング

ウ. ハンドオーバー

エ. MNP

解答・解説 正答：ウ

ア：契約事業者以外のネットワークなどを利用して通信する仕組みです。

イ：スマートフォンなどを他端末のインターネット接続手段として使う機能です。

ウ：端末の移動に合わせて接続する基地局を切り替え、通信継続を支えます。

エ：電話番号を維持して通信事業者を変更する制度です。

総合解説：ハンドオーバーは移動体通信で、端末の移動中も通信を続けるための重要な仕組みです。

問題 0060 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：標準

海外などで、自分が契約する通信事業者以外の提携ネットワークを利用して通信する仕組みはどれか。

ア. ハンドオーバー

イ. MNP

ウ. NTP

エ. ローミング

解答・解説 正答：エ

ア：移動中に基地局を切り替える仕組みです。

イ：電話番号を維持して事業者を変更する制度です。

ウ：時刻同期のプロトコルです。

エ：契約事業者のサービスエリア外などで他社ネットワークを利用する仕組みです。

総合解説：ローミングとハンドオーバーはどちらもモバイル関連用語ですが、意味が異なります。

問題 0061 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：標準

スマートフォンのモバイル回線を使い、ノートPCをインターネットへ接続する機能はどれか。

ア. テザリング

イ. MNP

ウ. ハンドオーバー

エ. DNS

解答・解説

正答：ア

ア：スマートフォンなどを通信の中継点として他端末へ接続を提供します。

イ：電話番号を維持して事業者を変更する制度です。

ウ：基地局の切替えです。

エ：名前解決の仕組みです。

総合解説：テザリングは外出先でPCなどをモバイル回線へ接続する際に利用されます。

問題 0062 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：標準

物理的なSIMカードを差し替えず、端末内蔵のSIM機能へ契約情報を設定できる仕組みはどれか。

ア. MIMO

イ. eSIM

ウ. RSS

エ. MIME

解答・解説

正答：イ

ア：複数アンテナを利用する通信技術です。

イ：eSIMは端末に組み込まれたSIM機能へ通信事業者の情報を設定して利用します。

ウ：Webサイトの更新情報配信などに使われます。

エ：電子メールで多様なデータを扱うための仕組みです。

総合解説：モバイル通信ではSIMカード、eSIM、MNP、テザリングなどの基本用語を理解します。

問題 0063 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：標準

電池で動作するセンサーから少量のデータを遠距離へ送るIoT用途で、低消費電力を重視した通信方式はどれか。

ア. HDMI

イ. USB

ウ. LPWA

エ. NFCだけ

解答・解説

正答：ウ

ア：映像・音声用の有線インタフェースです。

イ：周辺機器接続の有線規格です。

ウ：LPWAはLow Power Wide Areaで、低消費電力・広域通信を特徴とするIoT向け通信方式です。

エ：ごく近距離通信向けで、遠距離IoT用途とは異なります。

総合解説：IoT通信では通信距離、速度、消費電力などの要件に応じて方式を選びます。

問題 0064 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：応用

近距離で比較的低消費電力の無線通信を行い、ビーコンやセンサーなどで利用される技術はどれか。

ア. LPWA

イ. 光通信

ウ. SMTP

エ. BLE

解答・解説

正答：エ

ア：広域・低消費電力のIoT通信で利用されます。

イ：光ファイバーなどを利用する高速通信です。

ウ：メール送信プロトコルです。

エ：BLEはBluetooth Low Energyで、低消費電力の近距離通信に向きます。

総合解説：BLEとLPWAはどちらもIoTで利用されますが、通信距離や用途が異なります。

問題 0065 [6-2 ネットワーク] > [インターネット・無線・モバイル・IoT通信] ｜ 難易度：応用

工場内の短距離センサー通信と、広い農地に置く電池駆動センサーの通信方式を選ぶ。考え方として最も適切なものはどれか。

ア. 通信距離、必要速度、消費電力を比較し、短距離ならBLE、広域低消費電力ならLPWAなどを検討する。

イ. すべてのIoT機器で必ず同じ通信方式だけを使う。

ウ. 消費電力を考えず常に最速方式だけを選ぶ。

エ. 通信距離を確認せず近距離方式だけを使う。

解答・解説 正答：ア

ア：IoTネットワークは用途ごとの通信距離、速度、消費電力などを基に選定します。

イ：要件に合わない場合があります。

ウ：電池駆動機器では不適切な場合があります。

エ：遠距離機器へ届かない可能性があります。

総合解説：IoT通信では、一つの性能だけでなく距離・速度・消費電力などのバランスで方式を選びます。

問題 0066 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：基礎

企業における情報資産の例として、最も適切なものはどれか。

ア. 机の色だけ

イ. 顧客情報、営業情報、知的財産関連情報、人事情報など。

ウ. 空調の設定温度だけ

エ. キーボードのキー数だけ

解答・解説 正答：イ

ア：業務上保護すべき情報資産の代表例ではありません。

イ：企業活動で価値を持ち、保護対象となる情報は情報資産に含まれます。

ウ：状況により管理情報にはなり得ますが、設問の代表的な情報資産例ではありません。

エ：情報資産の代表例ではありません。

総合解説：情報セキュリティでは、まず組織にとって守るべき情報資産を把握することが重要です。

問題 0067 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：基礎

許可された者だけが情報へアクセスできるようにする性質はどれか。

ア. 完全性

イ. 可用性

ウ. 機密性

エ. 信頼性だけ

解答・解説 正答：ウ

ア：情報が正確で、不正に変更・破壊されていない性質です。

イ：必要なときに情報やシステムを利用できる性質です。

ウ：機密性は、権限のない者への情報開示を防ぐ性質です。

エ：情報セキュリティのCIAの一要素を表す用語ではありません。

総合解説：情報セキュリティの基本要素として、機密性・完全性・可用性を区別します。

問題 0068 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：基礎

情報が正確であり、不正に改ざんや破壊をされていない状態を保つ性質はどれか。

ア. 機密性

イ. 可用性

ウ. 可搬性

エ. 完全性

解答・解説 正答：エ

ア：許可された者だけが情報へアクセスできる性質です。

イ：必要なときに利用できる性質です。

ウ：他の環境へ移しやすい性質などを指します。

エ：完全性は情報の正確性や完全な状態を維持する性質です。

総合解説：完全性が失われると、データが改ざんされたり誤った内容になったりする可能性があります。

問題 0069 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：標準

災害や障害が発生しても、必要なときにシステムや情報を利用できるようにする性質はどれか。

ア. 可用性

イ. 機密性

ウ. 完全性

エ. 否認防止

解答・解説

正答：ア

ア：可用性は、必要な利用者が必要なときに情報やシステムを利用できる性質です。

イ：不正な開示を防ぐ性質です。

ウ：改ざんや破壊を防ぎ正確性を保つ性質です。

エ：行為を後から否認できないようにする性質です。

総合解説：可用性はバックアップや冗長化などとも関係する重要なセキュリティ要素です。

問題 0070 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：標準

顧客名簿が権限のない社員に閲覧された。最も直接的に損なわれた情報セキュリティの要素はどれか。

ア. 完全性

イ. 機密性

ウ. 可用性

エ. 性能

解答・解説

正答：イ

ア：データが改ざんされたことを示す事例ではありません。

イ：権限のない者に情報が開示されたため、機密性の問題です。

ウ：利用不能になったことを示す事例ではありません。

エ：情報セキュリティのCIAとは異なる観点です。

総合解説：事例では、漏えいは機密性、改ざんは完全性、利用不能は可用性と対応付けると整理しやすくなります。

問題 0071 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：標準

売上データが第三者によって書き換えられ、金額が正しくなくなった。最も直接的に損なわれた要素はどれか。

ア. 機密性

イ. 可用性

ウ. 完全性

エ. スループット

解答・解説

正答：ウ

ア：閲覧権限のない者への開示を示す事例ではありません。

イ：利用できないことを示す事例ではありません。

ウ：情報の正確性が失われているため、完全性の問題です。

エ：システム性能の指標です。

総合解説：完全性は情報が正確で改ざんされていないことを維持する性質です。

問題 0072 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：標準

攻撃によりオンラインサービスが停止し、正規利用者がアクセスできなくなった。最も直接的に損なわれた要素はどれか。

ア. 機密性

イ. 完全性

ウ. 著作権

エ. 可用性

解答・解説

正答：エ

ア：情報漏えいの有無を示す事例ではありません。

イ：データ改ざんの有無を示す事例ではありません。

ウ：知的財産権に関する概念です。

エ：正規利用者が必要なサービスを利用できないため、可用性が損なわれています。

総合解説：サービス停止やシステム利用不能は、可用性に関する代表的な問題です。

問題 0073 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：標準

セキュリティインシデントが発生しやすくなる、システムや組織上の弱点を何というか。

ア. 脆弱性

イ. 情報資産

ウ. 脅威

エ. 監査証拠

解答・解説 正答：ア

ア：脆弱性は攻撃や事故によって悪用され得る弱点です。

イ：組織が守るべき価値ある情報などです。

ウ：情報資産へ損害を与える可能性のある要因です。

エ：監査結論を裏付ける情報です。

総合解説：脆弱性にはソフトウェアの欠陥だけでなく、ルール未整備や教育不足など人的・組織的な弱点も含まれます。

問題 0074 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：応用

セキュリティ規程はあるが、従業員へ周知されず、パスワードを付箋に書いて端末へ貼る行為が常態化している。この状態として最も適切なものはどれか。

ア. 可用性が必ず100%確保されている。

イ. 人的脆弱性が存在する。

ウ. データベースが正規化されている。

エ. ネットワーク速度が向上している。

解答・解説 正答：イ

ア：人的脆弱性とは関係ありません。

イ：ルールや教育が徹底されず、不適切な行動が発生しやすい状態は人的脆弱性と考えられます。

ウ：DB設計の話で、セキュリティ行動とは異なります。

エ：通信性能とは関係ありません。

総合解説：脆弱性はシステムのバグだけでなく、人や組織の行動・ルールにも存在します。

問題 0075 [6-3 セキュリティ基礎・脅威] > [情報資産・機密性・完全性・可用性・脆弱性] ｜ 難易度：応用

従業員が会社の承認を得ず、個人契約のクラウドサービスへ業務データを保存している。この問題に最も関連する用語はどれか。

ア. VLAN

イ. レプリケーション

ウ. シャドーIT

エ. 正規化

解答・解説 正答：ウ

ア：LANを論理的に分割する技術です。

イ：データの複製を保持する仕組みです。

ウ：組織の管理部門が把握・承認していないITサービスや機器を業務で利用することを指します。

エ：DBの重複や更新不整合を減らす設計上の考え方です。

総合解説：シャドーITは情報漏えいや管理不能などのリスクにつながるため、組織として把握・管理する必要があります。

問題 0076 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：基礎

他のプログラムやファイルへ寄生するなどして感染を広げる不正プログラムとして代表的なものはどれか。

ア. ファイアウォール

イ. DBMS

ウ. NTP

エ. コンピュータウイルス

解答・解説 正答：エ

ア：通信を制御するセキュリティ対策です。

イ：データベース管理ソフトです。

ウ：時刻同期プロトコルです。

エ：コンピュータウイルスは代表的なマルウェアの一種です。

総合解説：マルウェアにはウイルス、ワーム、トロイの木馬、ランサムウェアなど複数の種類があります。

問題 0077 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：基礎

ファイルを暗号化するなどして利用できなくし、復旧と引換えに金銭を要求するマルウェアはどれか。

ア. ランサムウェア

イ. スパイウェア

ウ. キーロガー

エ. ファイアウォール

解答・解説

正答：ア

ア：ランサムウェアはデータやシステムを利用不能にして身代金を要求するマルウェアです。

イ：利用者の情報をひそかに収集するマルウェアです。

ウ：キー入力を記録する不正プログラムです。

エ：通信制御を行う対策です。

総合解説：ランサムウェアでは暗号化だけでなく、情報窃取と公開を組み合わせる二重脅迫が行われることもあります。

問題 0078 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：基礎

他のファイルへ寄生しなくても、ネットワークなどを介して自律的に複製・拡散する性質を持つマルウェアはどれか。

ア. トロイの木馬

イ. ワーム

ウ. スパイウェア

エ. プロキシ

解答・解説

正答：イ

ア：有用なプログラムなどを装って侵入するタイプのマルウェアです。

イ：ワームは自ら複製し、ネットワークなどを通じて拡散するマルウェアです。

ウ：情報をひそかに収集するマルウェアです。

エ：通信を中継する仕組みです。

総合解説：ワームは自己増殖・拡散する性質が特徴です。

問題 0079 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：標準

便利なソフトウェアを装って利用者に実行させ、裏で不正な処理を行うマルウェアはどれか。

ア. ワーム

イ. NTP

ウ. トロイの木馬

エ. VLAN

解答・解説

正答：ウ

ア：自己増殖して拡散する性質が代表的です。

イ：時刻同期プロトコルです。

ウ：正規・有用なプログラムのように見せかけて侵入することが特徴です。

エ：LANを論理的に分割する技術です。

総合解説：マルウェアは感染・侵入方法や目的によって種類を区別します。

問題 0080 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：標準

利用者がキーボードから入力した文字を記録し、IDやパスワードなどを盗み取るために悪用されるものはどれか。

ア. バックアップソフト

イ. スイッチ

ウ. DNS

エ. キーロガー

解答・解説

正答：エ

ア：データの複製を保存するソフトウェアです。

イ：LAN内の通信を転送する装置です。

ウ：名前解決の仕組みです。

エ：キー入力を記録することで認証情報などを盗むことがあります。

総合解説：キーロガーは技術的脅威の一つで、認証情報窃取に悪用されます。

問題 0081 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：標準

技術的な脆弱性ではなく、人の心理や不注意を利用して秘密情報を聞き出す手法はどれか。

ア. ソーシャルエンジニアリング

イ. SQLインジェクション

ウ. DDoS

エ. レプリケーション

解答・解説 正答：ア

ア：人の心理的な隙や行動を利用して情報を得る手法です。

イ：Webアプリケーションへの技術的な攻撃手法です。

ウ：大量通信などでサービスを妨害する攻撃です。

エ：データを複製する仕組みです。

総合解説：情報セキュリティでは、技術だけでなく人を狙う攻撃にも注意が必要です。

問題 0082 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：標準

攻撃者が取引先や経営者になりすましたメールを送り、担当者に偽の口座へ送金させる詐欺はどれか。

ア. デッドロック

イ. ビジネスメール詐欺（BEC）

ウ. VLAN

エ. MIMO

解答・解説 正答：イ

ア：DB処理が互いに待ち続ける状態です。

イ：BECはBusiness Email Compromiseで、メールを悪用して送金や情報提供をだまし取る攻撃です。

ウ：LANを論理分割する技術です。

エ：複数アンテナを利用する無線技術です。

総合解説：BECでは組織内外の関係者になりすますなど、人の判断を狙う点が特徴です。

問題 0083 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：応用

退職予定の社員が、業務上アクセスできる顧客情報を無断で持ち出した。脅威の分類として最も適切なものはどれか。

ア. 自然災害

イ. SQLインジェクション

ウ. 内部不正

エ. ハンドオーバー

解答・解説 正答：ウ

ア：物理的脅威の一つです。

イ：外部からWebアプリケーションを狙う代表的な技術的攻撃です。

ウ：組織内部の権限を持つ者などによる意図的な不正行為です。

エ：モバイル通信の基地局切替えです。

総合解説：情報セキュリティでは外部攻撃だけでなく、内部者による不正や誤操作も脅威として考えます。

問題 0084 [6-3 セキュリティ基礎・脅威] > [マルウェア・人的脅威・ソーシャルエンジニアリング] ｜ 難易度：応用

「社員の誤操作」「ランサムウェア」「地震による設備損壊」の分類として最も適切なものはどれか。

ア. 順に、物理的脅威・人的脅威・技術的脅威。

イ. すべて技術的脅威。

ウ. すべて人的脅威。

エ. 順に、人的脅威・技術的脅威・物理的脅威。

解答・解説 正答：エ

ア：分類が入れ替わっています。

イ：誤操作や地震は技術的脅威ではありません。

ウ：マルウェアや地震は人的脅威ではありません。

エ：誤操作は人、マルウェアは技術、災害は物理的要因による脅威です。

総合解説：脅威を人的・技術的・物理的に分類すると、必要な対策を考えやすくなります。

問題 0085 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：基礎

考えられる文字列の組合せを次々に試してパスワードを破ろうとする攻撃はどれか。

ア. 総当たり（ブルートフォース）攻撃

イ. パスワードリスト攻撃

ウ. SQLインジェクション

エ. DDoS

解答・解説

正答：ア

ア：多数の候補を網羅的に試行するパスワード攻撃です。

イ：他サービスなどから漏えいしたID・パスワードの組を試す攻撃です。

ウ：不正なSQLによりDB操作を狙う攻撃です。

エ：大量通信でサービス妨害を狙う攻撃です。

総合解説：パスワード攻撃には総当たり、辞書、パスワードリスト攻撃などがあります。

問題 0086 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：基礎

他のサービスから漏えいしたIDとパスワードの組合せを使い回し、別サービスへの不正ログインを試みる攻撃はどれか。

ア. 辞書攻撃

イ. パスワードリスト攻撃

ウ. DoS攻撃

エ. クリックジャッキング

解答・解説

正答：イ

ア：辞書にある単語などをパスワード候補として試します。

イ：漏えい済みの認証情報を別サービスへ試す攻撃で、クレデンシャルスタッフィングとも呼ばれます。

ウ：サービス提供を妨害する攻撃です。

エ：利用者をだまして意図しないクリックをさせる攻撃です。

総合解説：パスワードの使い回しは、パスワードリスト攻撃の被害を拡大させる要因になります。

問題 0087 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：基礎

Webアプリケーションの入力欄などへ不正な文字列を送り、意図しないデータベース操作を実行させようとする攻撃はどれか。

ア. クロスサイトスクリプティング

イ. DDoS

ウ. SQLインジェクション

エ. IPスプーフィング

解答・解説 正答：ウ

ア：Webページへ不正なスクリプトを混入させる攻撃です。

イ：大量の通信でサービスを妨害する攻撃です。

ウ：入力値を通じて不正なSQLを実行させ、DBの閲覧・改ざんなどを狙う攻撃です。

エ：IPアドレスを偽装する攻撃です。

総合解説：SQLインジェクションはWebアプリケーションを介してデータベースを狙う代表的な攻撃です。

問題 0088 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：標準

Webページへ悪意あるスクリプトを埋め込み、そのページを閲覧した利用者のブラウザ上で実行させる攻撃はどれか。

ア. SQLインジェクション

イ. DDoS

ウ. DNSキャッシュポイズニング

エ. クロスサイトスクリプティング（XSS）

解答・解説 正答：エ

ア：DBへ不正なSQLを実行させる攻撃です。

イ：大量通信によるサービス妨害です。

ウ：DNSのキャッシュへ偽情報を混入させる攻撃です。

エ：Webページへ不正なスクリプトを混入させ、利用者側で実行させる攻撃です。

総合解説：XSSはWeb利用者のブラウザ上で不正スクリプトを動作させる点が特徴です。

問題 0089 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：標準

ログイン済み利用者のブラウザを悪用し、利用者が意図しない送金や設定変更などのリクエストを送らせる攻撃はどれか。

ア. クロスサイトリクエストフォージェリ（CSRF）

イ. XSS

ウ. ブルートフォース攻撃

エ. ポートスキャン

解答・解説 正答：ア

ア：認証済み利用者の権限を悪用して、意図しないリクエストを送信させます。

イ：不正スクリプトを利用者のブラウザで実行させる攻撃です。

ウ：多数のパスワード候補を試す攻撃です。

エ：開いているポートなどを調べる攻撃準備の手法です。

総合解説：CSRFは、利用者が正規サイトへログイン済みであることを悪用するWeb攻撃です。

問題 0090 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：標準

多数の機器から大量の通信を送り付け、サービスを利用しにくくする攻撃はどれか。

ア. DoS攻撃（単一または限定的な送信元から行うサービス妨害）

イ. DDoS攻撃（多数の分散した機器から行うサービス妨害）

ウ. SQLインジェクション（不正なSQLでデータベース操作を狙うWeb攻撃）

エ. フィッシング（偽サイトなどで認証情報をだまし取る詐欺）

解答・解説 正答：イ

ア：サービス妨害という目的は同じですが、DDoSは多数の分散した送信元を利用する点が特徴です。

イ：複数の送信元から大量の通信を発生させ、サービス提供を妨害します。

ウ：DB操作を狙うWeb攻撃です。

エ：偽サイトなどで認証情報をだまし取る攻撃です。

総合解説：DDoSはDistributed Denial of Serviceで、可用性を狙う代表的な攻撃です。

問題 0091 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：標準

通信する二者の間へ攻撃者が入り込み、双方になりすまして通信内容を盗聴・改ざんする攻撃はどれか。

ア. 辞書攻撃

イ. クリプトジャッキング

ウ. 中間者攻撃

エ. ワンクリック詐欺

解答・解説 正答：ウ

ア：辞書にある単語などをパスワード候補として試す攻撃です。

イ：他人の計算資源を暗号資産の採掘などへ無断利用する攻撃です。

ウ：攻撃者が通信経路の途中へ入り、通信を傍受・改ざんします。

エ：利用者をだまして料金請求などを行う詐欺です。

総合解説：中間者攻撃は通信経路へ介在し、盗聴や改ざんを行うネットワーク攻撃です。

問題 0092 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：応用

銀行を装った偽サイトへ誘導して認証情報を入力させる攻撃をフィッシングという。SMSを利用して同様の誘導を行う手口はどれか。

ア. DDoS

イ. SQLインジェクション

ウ. バッファオーバーフロー

エ. スミッシング

解答・解説 正答：エ

ア：大量通信でサービスを妨害する攻撃です。

イ：DBへの不正操作を狙う攻撃です。

ウ：プログラムのメモリ領域を悪用する攻撃です。

エ：SMSとフィッシングを組み合わせた手口をスミッシングと呼びます。

総合解説：フィッシングは偽サイトなどへ誘導して情報を盗み、SMSを利用するものはスミッシングと呼ばれます。

問題 0093 [6-3 セキュリティ基礎・脅威] > [Web・ネットワーク・その他の攻撃手法] ｜ 難易度：応用

生成AIなどへの入力を悪用し、システムに本来意図しない指示を実行させようとする攻撃として、IPAシラバスVer.6.5に挙げられているものはどれか。

ア. プロンプトインジェクション攻撃

イ. データベース正規化

ウ. レスポンシブWebデザイン

エ. レプリケーション

解答・解説 正答：ア

ア：生成AI等への入力に悪意ある指示を混ぜ、本来の指示や制約を逸脱させようとする攻撃です。

イ：データ重複や更新不整合を減らす設計上の考え方です。

ウ：画面サイズに応じて表示を調整するWeb設計手法です。

エ：データの複製を保持する仕組みです。

総合解説：Ver.6.5の情報セキュリティ分野では、従来のWeb・ネットワーク攻撃に加え、プロンプトインジェクション攻撃も用語例に含まれています。

問題 0094 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：基礎

情報セキュリティのリスクマネジ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. 対応を先に決め、リスクの有無は確認しない。

イ. リスクの特定、分析、評価を行い、その結果に応じてリスク対応を決める。

ウ. 事故発生後だけリスクを考える。

エ. 情報資産を確認せず、全対策を同じ優先度で実施する。

解答・解説 正答：イ

ア：リスクを把握・評価してから対応を決めるのが基本です。

イ：IPAシラバスでは、リスクマネジメントを特定・分析・評価・対応という流れで捉えます。

ウ：事前の特定・評価と準備が重要です。

エ：リスクの大きさに応じて優先順位を付ける必要があります。

総合解説：リスクマネジメントでは、情報資産に対する脅威や脆弱性を把握し、リスクを評価した上で対応方法を選びます。

問題 0095 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：基礎

リスク特定、リスク分析、リスク評価をまとめて表す用語はどれか。

ア. リスク保有

イ. リスク回避

ウ. リスクアセスメント

エ. インシデント対応

解答・解説 正答：ウ

ア：評価したリスクを受け入れる対応です。

イ：リスクの原因となる活動を行わないなどの対応です。

ウ：リスクアセスメントは、リスクを見つけ、分析し、評価する一連の活動です。

エ：発生した事故への具体的な対応活動です。

総合解説：リスクアセスメントとリスク対応は区別し、まず評価してから対応を選択します。

問題 0096 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：基礎

情報資産に対して、どのような脅威や脆弱性が存在し、どのような損失が起こり得るかを洗い出す活動はどれか。

ア. リスク評価

イ. リスク保有

ウ. コミット

エ. リスク特定

解答・解説 正答：エ

ア：分析結果を基に、対応の必要性や優先度を判断する段階です。

イ：リスク対応の一つです。

ウ：DBのトランザクションを確定する操作です。

エ：リスク特定では、リスクの原因や対象、起こり得る事象を明らかにします。

総合解説：リスク特定は、リスクアセスメントの出発点となる活動です。

問題 0097 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：標準

ある脅威の発生可能性と、発生した場合の影響度を見積もった後、そのリスクを許容できるか、対策を優先すべきか判断する活動はどれか。

ア. リスク評価

イ. リスク特定

ウ. リスク分析

エ. リスク移転

解答・解説 正答：ア

ア：分析した結果を基に、受容可能性や優先順位を判断するのがリスク評価です。

イ：どのようなリスクが存在するかを洗い出す活動です。

ウ：発生可能性や影響などを見積もる活動です。

エ：保険などで損失負担を他者へ移す対応です。

総合解説：リスク分析で大きさを把握し、リスク評価で対応の必要性や優先度を判断します。

問題 0098 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：標準

重要情報を扱う危険性が高い外部サービスの利用そのものを中止する対応はどれか。

ア. リスク保有

イ. リスク回避

ウ. リスク移転

エ. リスク分散

解答・解説 正答：イ

ア：リスクを受け入れる対応です。

イ：リスクの原因となる活動をやめることで、該当リスクを避ける対応です。

ウ：損失負担を保険会社などへ移す対応です。

エ：対象を複数に分けて一か所への集中を避ける対応です。

総合解説：リスク対応には回避、共有、保有などがあり、リスクの性質や費用対効果に応じて選びます。

問題 0099 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：標準

サイバー事故による金銭的損失の一部に備えるため、サイバー保険へ加入する対応はどれか。

ア. リスク回避

イ. リスク保有

ウ. リスク移転

エ. リスク特定

解答・解説 正答：ウ

ア：リスクの原因となる活動をやめる対応です。

イ：リスクを受け入れる対応です。

ウ：保険契約などを通じて、損失の一部を他者へ移す対応です。

エ：リスクを洗い出す活動です。

総合解説：リスク共有にはリスク移転やリスク分散などの考え方があります。

問題 0100 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：標準

発生可能性も影響も小さく、対策費用の方が大きいと判断したリスクを、組織が認識した上で受け入れる対応はどれか。

ア. リスク回避

イ. リスク移転

ウ. リスク分析

エ. リスク保有

解答・解説 正答：エ

ア：原因となる活動をやめる対応です。

イ：損失負担を他者へ移す対応です。

ウ：リスクの大きさを見積もる活動です。

エ：リスクを把握・評価した上で、そのまま受け入れる対応です。

総合解説：すべてのリスクをゼロにするのではなく、許容水準に応じてリスク保有を選ぶ場合もあります。

問題 0101 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：応用

想定損失が小さいリスクに対し、非常に高額な対策を導入する案が出た。適切な考え方はどれか。

ア. リスクの大きさ、許容水準、対策費用を比較し、費用対効果を考えて対応を決める。

イ. リスクの大小に関係なく最も高価な対策を必ず導入する。

ウ. 対策費だけを見て全てのリスクを無視する。

エ. 事故が起きるまでリスクを評価しない。

解答・解説 正答：ア

ア：セキュリティ対策は、リスク低減効果と必要コストを総合して決める必要があります。

イ：過剰投資となる場合があります。

ウ：重大なリスクを放置する可能性があります。

エ：事前評価と準備が重要です。

総合解説：リスク対応では、リスクレベルと対策コスト、事業への影響を総合して優先順位を決めます。

問題 0102 [6-4 情報セキュリティ管理] > [リスクアセスメント・リスク対応] ｜ 難易度：応用

サイバー攻撃による情報漏えいが起きた場合に備え、平常時に実施すべき対応として最も適切なものはどれか。

ア. 事故発生時に初めて担当者を決める。

イ. 対応マニュアルを整備し、連絡体制を決め、定期的に教育・訓練を行う。

ウ. 連絡先や判断基準を文書化しない。

エ. 訓練を行わず、手順が実行可能か確認しない。

解答・解説 正答：イ

ア：対応が遅れる可能性があります。

イ：事故発生時に迅速に行動できるよう、事前の手順整備と訓練が必要です。

ウ：緊急時に混乱しやすくなります。

エ：手順の実効性を検証できません。

総合解説：リスクマネジメントでは事故の予防だけでなく、発生時の対応準備も重要です。

問題 0103 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：基礎

組織が情報セキュリティを継続的・体系的に管理するための仕組みはどれか。

ア. DBMS

イ. DNS

ウ. ISMS

エ. DLP

解答・解説 正答：ウ

ア：データベースを管理するシステムです。

イ：名前解決の仕組みです。

ウ：ISMSはInformation Security Management Systemで、組織的に情報セキュリティを管理する仕組みです。

エ：情報漏えい防止に用いられる技術的対策です。

総合解説：ISMSは単発の対策ではなく、方針、リスク管理、対策、評価、改善を継続して行う考え方です。

問題 0104 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：基礎

組織として情報セキュリティにどのように取り組むかという基本方針を示すものはどれか。

ア. E-R図

イ. WBS

ウ. ベンチマーク

エ. 情報セキュリティポリシー

解答・解説 正答：エ

ア：データベースの実体と関連を表す図です。

イ：プロジェクト作業を分解した構成です。

ウ：性能比較などに使う評価方法です。

エ：組織の情報セキュリティに関する基本方針や考え方を示します。

総合解説：情報セキュリティポリシーは、組織内で対策を一貫して進めるための基礎になります。

問題 0105 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：基礎

情報セキュリティ対策を計画し、実施し、評価し、改善するサイクルとして代表的なものはどれか。

ア. PDCA

イ. FIFO

ウ. OSI

エ. LATCH

解答・解説

正答：ア

ア：Plan、Do、Check、Actを繰り返し、継続的に改善します。

イ：キューの処理方式です。

ウ：ネットワークの参照モデルです。

エ：情報整理の原則です。

総合解説：ISMSでは、状況の変化に合わせて管理策を見直し、継続的改善を行うことが重要です。

問題 0106 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：標準

情報漏えい、マルウェア感染、サービス停止など、情報セキュリティ上の望ましくない事象を何というか。

ア. トランザクション

イ. 情報セキュリティインシデント

ウ. リレーション

エ. スループット

解答・解説

正答：イ

ア：DBの一連の処理単位です。

イ：セキュリティを損なう、またはその可能性がある事象を指します。

ウ：関係データベースの表などを表す概念です。

エ：単位時間当たりの処理量です。

総合解説：インシデントを適切に検知・報告・対応できる体制を整えることが重要です。

問題 0107 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：標準

経営層、情報システム部門、利用部門などの関係者が、セキュリティリスクに関する情報を共有し、認識を合わせる活動はどれか。

ア. リスク回避

イ. データベース結合

ウ. リスクコミュニケーション

エ. ルーティング

解答・解説 正答：ウ

ア：リスク原因となる活動をやめる対応です。

イ：複数の表を関連付ける操作です。

ウ：リスクについて関係者間で情報交換し、共通認識を形成する活動です。

エ：ネットワーク上の経路を選択する処理です。

総合解説：情報セキュリティは特定部門だけではなく、関係者間の情報共有と合意形成が重要です。

問題 0108 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：標準

情報や利用者が、本物であることを確認できる性質はどれか。

ア. 機密性

イ. 可用性

ウ. スループット

エ. 真正性

解答・解説 正答：エ

ア：権限のない者への情報開示を防ぐ性質です。

イ：必要なときに利用できる性質です。

ウ：処理性能の指標です。

エ：真正性は、情報の発信者や利用者などが確かに本人・本物であることを確かめられる性質です。

総合解説：情報セキュリティにはCIAに加えて、真正性、責任追跡性、否認防止、信頼性などの要素もあります。

問題 0109 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：標準

誰が、いつ、どの操作を行ったかをログなどから追跡できる性質はどれか。

ア. 責任追跡性

イ. 可用性

ウ. 機密性

エ. 圧縮率

解答・解説 正答：ア

ア：操作主体と行為を後から追跡できることを表します。

イ：必要時に利用できる性質です。

ウ：不正な開示を防ぐ性質です。

エ：データ圧縮に関する指標です。

総合解説：ログ管理などは、事故調査や不正行為の追跡に役立ちます。

問題 0110 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：標準

送信者が後から『そのメッセージは自分が送っていない』と主張することを防ぐために重視される性質はどれか。

ア. 可用性

イ. 否認防止

ウ. 機密性

エ. 冗長性

解答・解説 正答：イ

ア：必要時に利用できる性質です。

イ：行為を後から否定できないよう証拠を残す性質です。

ウ：情報を秘密に保つ性質です。

エ：複数構成によって故障に備える考え方です。

総合解説：否認防止にはデジタル署名などの技術が活用されます。

問題 0111 [6-4 情報セキュリティ管理] > [ISMS・セキュリティポリシー] ｜ 難易度：応用

新たなクラウドサービス導入後、情報セキュリティ管理を継続的に改善する対応として最も適切なものはどれか。

ア. 一度決めた対策は環境が変わっても永久に見直さない。

イ. セキュリティポリシーを作成した時点で管理活動を終了する。

ウ. リスクを再評価し、必要な管理策を実施し、結果を評価して方針や手順を見直す。

エ. 事故が起きても記録や評価を行わない。

解答・解説 正答：ウ

ア：新たな脅威や業務変化に対応できません。

イ：継続的な運用と改善が必要です。

ウ：環境変化に応じてリスクと対策を見直すことがISMSの継続的改善につながります。

エ：再発防止や改善につながりません。

総合解説：ISMSでは、リスクマネジメントとPDCAを組み合わせ、組織としてセキュリティを継続的に改善します。

問題 0112 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：基礎

組織内でセキュリティインシデントの受付、分析、対応調整、再発防止などを担うチームはどれか。

ア. SOC

イ. DBA

ウ. PMO

エ. CSIRT

解答・解説 正答：エ

ア：監視・分析を継続的に行う組織として代表的です。

イ：データベース管理者です。

ウ：プロジェクト管理を支援する組織です。

エ：CSIRTはComputer Security Incident Response Teamで、インシデント対応を専門的に行う組織です。

総合解説：CSIRTは発生したセキュリティインシデントへの組織的な対応を担います。

問題 0113 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：基礎

ネットワークやシステムのログ・アラートを継続的に監視し、サイバー攻撃の兆候を分析する組織はどれか。

ア. SOC

イ. CSIRT

ウ. CA

エ. ISP

解答・解説 正答：ア

ア：SOCはSecurity Operation Centerで、セキュリティ監視・分析を行います。

イ：インシデント発生時の対応調整などを主に担います。

ウ：デジタル証明書を発行・管理する認証局です。

エ：インターネット接続サービス事業者です。

総合解説：SOCとCSIRTは連携することが多く、SOCは監視・検知、CSIRTは対応調整という役割で整理できます。

問題 0114 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：基礎

組織全体の情報セキュリティ方針や重要事項を検討し、部門横断で対策を推進するために設置される組織として最も適切なものはどれか。

ア. DNSサーバ

イ. 情報セキュリティ委員会

ウ. プロキシ

エ. DBMS

解答・解説 正答：イ

ア：名前解決を行うシステムです。

イ：情報セキュリティに関する方針や重要課題を組織横断で検討するために設置されます。

ウ：通信を中継する仕組みです。

エ：データベース管理システムです。

総合解説：情報セキュリティ管理では、経営層や各部門を含む組織的な体制が重要です。

問題 0115 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：標準

24時間ログを監視して不審な通信を発見する担当と、発見後に関係部署と連携して封じ込めや復旧を進める担当の組合せとして最も適切なものはどれか。

ア. 監視・分析はCSIRTだけ、対応調整はDNS。

イ. 監視・分析はCA、対応調整はDBMS。

ウ. 監視・分析はSOC、インシデント対応調整はCSIRT。

エ. 両方ともプリンターが担当する。

解答・解説 正答：ウ

ア：DNSは名前解決の仕組みです。

イ：いずれも役割が異なります。

ウ：SOCは継続的監視、CSIRTはインシデント対応を担う代表的な役割です。

エ：プリンターは出力装置です。

総合解説：SOCとCSIRTの役割を区別しつつ、実際の組織では相互に連携することが重要です。

問題 0116 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：標準

中小企業が自ら情報セキュリティ対策に取り組むことを自己宣言するIPAの制度はどれか。

ア. ISMAP

イ. J-CSIP

ウ. PCI DSS

エ. SECURITY ACTION

解答・解説 正答：エ

ア：政府情報システム向けクラウドサービスのセキュリティ評価制度です。

イ：標的型攻撃等の情報共有を行う取組です。

ウ：クレジットカード情報保護に関するセキュリティ基準です。

エ：SECURITY ACTIONは、中小企業が情報セキュリティ対策への取組を自己宣言する制度です。

総合解説：SECURITY ACTIONは中小企業が基本的な情報セキュリティ対策に取り組むきっかけとなる自己宣言制度です。

問題 0117 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：標準

政府が利用するクラウドサービスについて、セキュリティ要求への対応状況を評価・登録する制度はどれか。

ア. ISMAP

イ. SECURITY ACTION

ウ. J-CRAT

エ. MNP

解答・解説 正答：ア

ア：ISMAPは政府情報システムのためのセキュリティ評価制度です。

イ：中小企業の情報セキュリティ対策自己宣言制度です。

ウ：サイバー攻撃被害組織への支援を行う取組です。

エ：携帯電話番号を維持して事業者を変更する制度です。

総合解説：ISMAPは政府によるクラウドサービス利用時のセキュリティ確保を目的とした制度です。

問題 0118 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：標準

参加組織間でサイバー攻撃に関する情報を共有し、早期対応や被害拡大防止へ役立てるIPAの取組はどれか。

ア. J-CRAT

イ. J-CSIP

ウ. ISMAP

エ. CSMA/CD

解答・解説 正答：イ

ア：サイバー攻撃被害へのレスキュー活動を行います。

イ：J-CSIPはサイバー情報共有イニシアティブで、参加組織間の情報共有を行います。

ウ：政府向けクラウドサービスの評価制度です。

エ：LANで用いられたアクセス制御方式です。

総合解説：攻撃情報の共有は、他組織での早期検知や被害予防に役立ちます。

問題 0119 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：標準

経営者のリーダーシップの下でサイバーセキュリティ対策を推進する考え方を示す経済産業省・IPAのガイドラインはどれか。

ア. 中小企業の情報セキュリティ対策ガイドライン

イ. PCI DSS

ウ. サイバーセキュリティ経営ガイドライン

エ. OSI基本参照モデル

解答・解説 正答：ウ

ア：中小企業向けに具体的な対策を示すIPAのガイドラインです。

イ：クレジットカード情報を保護するためのセキュリティ基準です。

ウ：経営課題としてサイバーセキュリティへ取り組むための考え方や経営者向け指針を示します。

エ：通信機能を7層に整理したモデルです。

総合解説：サイバーセキュリティ経営ガイドラインは、サイバーリスクを経営課題として扱い、経営者が主導して対策することを重視します。

問題 0120 [6-4 情報セキュリティ管理] > [CSIRT・SOC・関連制度・ガイドライン] ｜ 難易度：応用

中小企業が基本的な情報セキュリティ対策を具体的に進めたい。参照先として最も適切なものはどれか。

ア. OSI基本参照モデル

イ. E-R図

ウ. PPM

エ. 中小企業の情報セキュリティ対策ガイドライン

解答・解説 正答：エ

ア：ネットワーク通信の階層モデルです。

イ：データベース設計に使う図です。

ウ：事業ポートフォリオ分析です。

エ：中小企業が実践すべき基本的な情報セキュリティ対策を体系的に示しています。

総合解説：制度やガイドラインは目的が異なるため、自社の規模や目的に合うものを参照します。2026年には中小企業向けガイドライン第4.0版が公開されています。

問題 0121 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：基礎

標的型メール訓練や情報セキュリティ教育は、主にどの種類の対策に分類されるか。

ア. 従業員の知識・行動を改善する人的セキュリティ対策

イ. 建物や設備への接触を制限する物理的セキュリティ対策

ウ. 機器やソフトウェアで通信・端末を守る技術的セキュリティ対策

エ. データベース設計で重複を減らす正規化

解答・解説 正答：ア

ア：教育や訓練は利用者の知識・行動を改善する人的対策です。

イ：入退室管理や施錠など施設・設備に関する対策です。

ウ：ファイアウォールや暗号化など技術を用いる対策です。

エ：DB設計上の対策で、セキュリティ対策分類とは異なります。

総合解説：人的対策では、教育・訓練、ルール遵守、適切なアクセス権運用などが重要です。

問題 0122 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：基礎

サーバ室への入退室をICカードで制限する対策は、主にどの種類に分類されるか。

ア. 研修やルール周知によって行動を改善する人的対策

イ. サーバ室への物理アクセスを制限する物理的対策

ウ. ファイアウォールなどで通信を制御する技術的対策

エ. 顧客獲得を目的とするマーケティング施策

解答・解説 正答：イ

ア：教育や訓練など、人の行動に関する対策です。

イ：施設や機器への物理的な接触を制限する対策です。

ウ：通信やシステムを技術で保護する対策です。

エ：情報セキュリティの分類ではありません。

総合解説：物理的対策には入退室管理、施錠、防犯カメラ、セキュリティケーブルなどがあります。

問題 0123 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：基礎

ファイアウォールやWAF、IDS、IPSなどは、主にどの種類の対策に分類されるか。

ア. 標的型メール訓練などで利用者を教育する人的対策

イ. 施錠や監視カメラで設備を守る物理的対策

ウ. 防御装置やソフトウェアを用いる技術的対策

エ. 会計処理の承認ルールを整える財務管理施策

解答・解説 正答：ウ

ア：教育や訓練などが該当します。

イ：施設や設備の物理的保護が該当します。

ウ：システムや通信を技術的な仕組みで保護する対策です。

エ：情報セキュリティ対策の分類ではありません。

総合解説：技術的対策にはアクセス制御、ファイアウォール、WAF、IDS/IPS、EDR、DLP、SIEMなどがあります。

問題 0124 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：標準

ネットワークの境界などで通信を監視し、許可された通信だけを通すために利用するものはどれか。

ア. WAF

イ. DLP

ウ. ICカード

エ. ファイアウォール

解答・解説 正答：エ

ア：Webアプリケーションへの攻撃対策に特化した仕組みです。

イ：機密情報の持出しや漏えい防止を支援する仕組みです。

ウ：認証や入退室管理などに使われます。

エ：通信元・宛先・ポートなどの条件に基づいて通信を制御します。

総合解説：ファイアウォールはネットワーク通信を制御する基本的な技術的対策です。

問題 0125 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：標準

SQLインジェクションやXSSなど、Webアプリケーションへの攻撃を検知・遮断するために利用されるものはどれか。

ア. WAF

イ. 一般的なファイアウォールだけ

ウ. NTP

エ. DNS

解答・解説

正答：ア

ア：WAFはWeb Application Firewallで、Webアプリケーション層の攻撃対策に用いられます。

イ：ネットワーク通信制御が中心で、Webアプリ攻撃への専用対策ではありません。

ウ：時刻同期プロトコルです。

エ：名前解決の仕組みです。

総合解説：WAFはWebアプリケーションを狙う代表的な攻撃への対策として利用されます。

問題 0126 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：標準

不審な通信を検知して通知する仕組みと、検知に加えて通信を遮断する仕組みの組合せとして最も適切なものはどれか。

ア. 検知はIPS、遮断はDNS。

イ. 検知はIDS、遮断まで行うのはIPS。

ウ. 検知はWAF、遮断はNTP。

エ. 両方ともバックアップ装置。

解答・解説

正答：イ

ア：DNSは名前解決の仕組みです。

イ：IDSは侵入検知、IPSは侵入防止を目的とします。

ウ：役割が異なります。

エ：ネットワーク監視・防御の仕組みです。

総合解説：IDSとIPSは名前が似ていますが、検知中心か防止まで行うかで区別します。

問題 0127 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：標準

PCやサーバなどのエンドポイント上の挙動を監視し、不審な活動の検知・調査・対応を支援する仕組みはどれか。

ア. DLP

イ. SIEM

ウ. EDR

エ. VPN

解答・解説 正答：ウ

ア：機密情報の漏えい防止に重点を置く仕組みです。

イ：複数機器のログを集約・分析する仕組みです。

ウ：EDRはEndpoint Detection and Responseで、端末上の不審な挙動の検知と対応を支援します。

エ：暗号化された仮想的な専用通信路を提供する仕組みです。

総合解説：EDRは従来型のマルウェア対策だけでは見つけにくい挙動も監視し、端末での調査・対応に役立ちます。

問題 0128 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：標準

機密情報がメールやUSBメモリなどを通じて外部へ持ち出されることを検知・制御する仕組みはどれか。

ア. EDR

イ. IDS

ウ. RAID

エ. DLP

解答・解説 正答：エ

ア：エンドポイントの不審挙動の検知・対応を支援します。

イ：ネットワーク上の侵入を検知する仕組みです。

ウ：記憶装置の冗長化技術です。

エ：DLPはData Loss Preventionで、重要情報の漏えいや不正持出しを防止するために利用されます。

総合解説：DLPは情報の内容や移動経路を監視し、重要データの流出防止に役立ちます。

問題 0129 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：応用

ファイアウォール、サーバ、認証システムなど複数の機器からログを集約し、相関分析して異常を発見したい。適した仕組みはどれか。

ア. SIEM

イ. EDRだけ

ウ. DLPだけ

エ. NTPだけ

解答・解説 正答：ア

ア：SIEMはSecurity Information and Event Managementで、複数のログを集約・分析します。

イ：主にエンドポイントの監視・対応を支援する仕組みです。

ウ：情報漏えい防止が主目的です。

エ：時刻同期を行うプロトコルです。

総合解説：SIEMは複数ソースのログを横断的に分析し、セキュリティ監視やインシデント調査を支援します。

問題 0130 [6-5 セキュリティ対策] > [人的・物理的・技術的対策] ｜ 難易度：応用

標的型攻撃への対策として最も適切な考え方はどれか。

ア. ウイルス対策ソフト一つだけで全ての攻撃を防げると考える。

イ. 教育・訓練、入退室管理、メール対策、EDR、アクセス制御など複数の対策を組み合わせる。

ウ. 技術対策だけ実施し、利用者教育を不要とする。

エ. セキュリティ対策を行わず、事故後だけ対応する。

解答・解説 正答：イ

ア：単一対策では防げない脅威があります。

イ：一つの対策だけに依存せず、人的・物理的・技術的対策を重ねることで被害を抑えやすくなります。

ウ：人的要因を狙う攻撃への備えが不足します。

エ：予防・検知・対応を組み合わせる必要があります。

総合解説：セキュリティ対策は多層的に組み合わせ、予防、検知、対応、復旧までを考えることが重要です。

問題 0131 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：基礎

第三者に内容を読まれにくくするため平文を別の形へ変換する処理を何というか。

ア. 復号

イ. ハッシュ化

ウ. 暗号化

エ. 圧縮

解答・解説 正答：ウ

ア：暗号文を元の平文へ戻す処理です。

イ：入力から固定長のハッシュ値を生成する処理です。

ウ：平文を鍵などを用いて暗号文へ変換する処理です。

エ：データ量を減らす処理です。

総合解説：暗号化と復号は、情報の機密性を確保する代表的な技術です。

問題 0132 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：基礎

暗号化と復号に同じ鍵を利用する方式はどれか。

ア. 公開鍵暗号方式

イ. ハッシュ関数

ウ. デジタル署名

エ. 共通鍵暗号方式

解答・解説 正答：エ

ア：暗号化と復号に異なる鍵の組を利用します。

イ：一方向性の要約値生成に用います。

ウ：本人性や改ざん検知に利用されます。

エ：送信者と受信者が同じ秘密鍵を共有して利用します。

総合解説：共通鍵暗号は高速に処理しやすい一方、鍵を安全に共有する必要があります。

問題 0133 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：基礎

公開してよい鍵と秘密に保つ鍵のペアを利用する暗号方式はどれか。

ア. 公開鍵暗号方式

イ. 共通鍵暗号方式

ウ. 可逆圧縮

エ. チェックディジット

解答・解説

正答：ア

ア：公開鍵と秘密鍵という異なる二つの鍵を組み合わせて利用します。

イ：暗号化と復号に同じ鍵を用います。

ウ：元データへ完全に戻せる圧縮方式です。

エ：入力誤り検出などに使う付加値です。

総合解説：公開鍵暗号方式は、鍵配送やデジタル署名などに利用されます。

問題 0134 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：標準

大量データ本体は共通鍵暗号で高速に暗号化し、その共通鍵を公開鍵暗号で安全に渡す方式はどれか。

ア. 共通鍵暗号方式だけ

イ. ハイブリッド暗号方式

ウ. ハッシュ方式

エ. 可逆圧縮

解答・解説

正答：イ

ア：共通鍵の安全な受渡しが別途必要です。

イ：共通鍵暗号の高速性と公開鍵暗号の鍵配送の利点を組み合わせます。

ウ：暗号化・復号を行う方式ではありません。

エ：データ量を減らす方式です。

総合解説：実際の安全な通信では、複数の暗号技術を組み合わせるハイブリッド方式が広く利用されます。

問題 0135 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：標準

任意長のデータから一定長の値を生成し、元データの改ざん検知などに利用されるものはどれか。

ア. 共通鍵暗号

イ. 公開鍵暗号

ウ. ハッシュ関数

エ. 圧縮アルゴリズム

解答・解説 正答：ウ

ア：鍵を使って暗号化・復号する方式です。

イ：公開鍵と秘密鍵を利用する暗号方式です。

ウ：入力データから固定長のハッシュ値を生成し、データが変わると通常ハッシュ値も変化します。

エ：データ量を削減する処理です。

総合解説：ハッシュ関数は一方向性を持つことが重要で、改ざん検知やパスワード保護などに利用されます。

問題 0136 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：標準

暗号化とハッシュ化の違いとして、最も適切なものはどれか。

ア. どちらも必ず元データへ復元できる。

イ. どちらも鍵を必ず一つ共有する。

ウ. ハッシュは動画再生専用技術である。

エ. 暗号化は鍵を用いて復号できることを前提とするが、ハッシュ化は元データへの復元を目的としない。

解答・解説 正答：エ

ア：ハッシュは復元を目的としません。

イ：ハッシュ関数は通常、共有鍵を必要としません。

ウ：改ざん検知など幅広い用途があります。

エ：暗号化は機密性確保のため復号を前提としますが、ハッシュは一方向の要約値生成を目的とします。

総合解説：暗号化とハッシュ化は目的と性質が異なるため、用途に応じて使い分けます。

問題 0137 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：標準

送信者本人が作成したことの確認と、送信後に内容が改ざんされていないことの確認に利用される技術はどれか。

ア. デジタル署名

イ. 共通鍵暗号だけ

ウ. 可逆圧縮

エ. VPN

解答・解説 正答：ア

ア：デジタル署名は本人性の確認と改ざん検知に利用され、否認防止にも役立ちます。

イ：送信者本人の証明や否認防止を直接実現する仕組みではありません。

ウ：データ量を減らす技術です。

エ：通信経路を保護する仕組みです。

総合解説：デジタル署名では、署名鍵と検証鍵を用いて署名を作成・検証します。

問題 0138 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：標準

デジタル署名で、署名者が署名を作成する際に使用し、他人に知られないよう管理すべき鍵はどれか。

ア. 検証鍵

イ. 署名鍵

ウ. 共通鍵

エ. SSID

解答・解説 正答：イ

ア：署名が正しいか確認するために利用され、公開して利用できます。

イ：署名鍵は署名者が秘密に保持し、署名作成に使用します。

ウ：共通鍵暗号で暗号化と復号に共有する鍵です。

エ：無線LANのネットワーク名です。

総合解説：署名鍵を秘密に保ち、検証鍵を用いて第三者が署名を確認できることがデジタル署名の基本です。

問題 0139 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：応用

機密文書を第三者に読まれないようにし、さらに送信者と改ざんの有無も確認したい。適切な考え方はどれか。

ア. デジタル署名だけで文書内容を必ず秘密にできる。

イ. 暗号化だけで送信者本人であることを必ず証明できる。

ウ. 文書を暗号化して機密性を確保し、デジタル署名で本人性と改ざんの有無を確認する。

エ. 圧縮だけで機密性と本人性を両方確保する。

解答・解説 正答：ウ

ア：デジタル署名の主目的は本人確認・改ざん検知で、機密性確保そのものではありません。

イ：暗号化だけでは署名者の証明を目的としません。

ウ：暗号化とデジタル署名は目的が異なるため、必要に応じて組み合わせます。

エ：圧縮はセキュリティ目的の技術ではありません。

総合解説：セキュリティ技術は、機密性、完全性、真正性など確保したい性質に合わせて組み合わせます。

問題 0140 [6-5 セキュリティ対策] > [暗号・ハッシュ・デジタル署名] ｜ 難易度：応用

暗号技術を安全に利用する際の考え方として、最も適切なものはどれか。

ア. 古い暗号方式でも一度導入したら永久に見直さない。

イ. 秘密鍵を全社員へ公開して管理を簡単にする。

ウ. 暗号化すればアクセス制御や認証は一切不要になる。

エ. 十分な強度を持つ方式と鍵長を選び、鍵を安全に管理し、必要に応じて更新する。

解答・解説 正答：エ

ア：技術進歩や脆弱性に応じて見直しが必要です。

イ：秘密鍵の漏えいは安全性を損ないます。

ウ：他のセキュリティ対策も必要です。

エ：暗号の安全性はアルゴリズムだけでなく、鍵長や鍵管理にも大きく左右されます。

総合解説：暗号技術は方式選定、鍵長、鍵の保管・更新などを含めて安全に運用する必要があります。

問題 0141 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：基礎

システムへアクセスしようとしている利用者が、本人であることを確認する仕組みはどれか。

ア. 利用者認証

イ. データ圧縮

ウ. レプリケーション

エ. ロードバランシング

解答・解説 正答：ア

ア：利用者認証は、アクセスしようとしている者の本人性を確認します。

イ：データ量を減らす処理です。

ウ：データを複製する仕組みです。

エ：処理負荷を複数装置へ分散します。

総合解説：利用者認証はアクセス制御の前提となる重要なセキュリティ機能です。

問題 0142 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：基礎

知識情報、所持情報、生体情報など異なる種類の認証要素を二つ以上組み合わせる方式はどれか。

ア. シングルサインオン

イ. 多要素認証

ウ. パスワードレス認証

エ. アクセス制御リスト

解答・解説 正答：イ

ア：一度の認証で複数サービスを利用しやすくする仕組みです。

イ：異なる要素を組み合わせることで、単一要素が破られた場合のリスクを低減します。

ウ：パスワードを使わない認証方式の総称です。

エ：資源へのアクセス権を定める仕組みです。

総合解説：多要素認証では、例えばパスワードとワンタイムパスワードなど異なる要素を組み合わせます。

問題 0143 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：標準

一度だけ、または短時間だけ有効なパスワードを使う認証方式はどれか。

ア. シングルサインオン

イ. 生体認証

ウ. ワンタイムパスワード

エ. IPフィルタリング

解答・解説 正答：ウ

ア：一回の認証で複数サービスを利用する仕組みです。

イ：身体的・行動的特徴を利用する認証です。

ウ：毎回異なる一時的なパスワードを使うことで、固定パスワードの漏えいリスクを低減します。

エ：IPアドレスに基づいて通信を制御する仕組みです。

総合解説：ワンタイムパスワードは多要素認証の一要素として利用されることがあります。

問題 0144 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：標準

一度の利用者認証で、複数の連携サービスへ繰り返しログインせず利用できる仕組みはどれか。

ア. 多要素認証

イ. ワンタイムパスワード

ウ. VPN

エ. シングルサインオン

解答・解説 正答：エ

ア：異なる種類の認証要素を組み合わせる方式です。

イ：一時的なパスワードを使う方式です。

ウ：仮想的な専用通信路を構築する仕組みです。

エ：一回の認証結果を複数の連携サービスで利用できる仕組みです。

総合解説：シングルサインオンは利便性を高める一方、認証基盤の保護が重要になります。

問題 0145 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：標準

本人であるにもかかわらず、認証システムが誤って本人ではないと判定する割合を何というか。

ア. 本人拒否率（FRR）

イ. 他人受入率（FAR）

ウ. 稼働率

エ. 圧縮率

解答・解説 正答：ア

ア：FRRはFalse Rejection Rateで、本人を誤って拒否する割合です。

イ：他人を誤って本人として受け入れる割合です。

ウ：システムが利用可能な時間の割合です。

エ：データ圧縮に関する指標です。

総合解説：生体認証ではFRRとFARのバランスを考慮する必要があります。

問題 0146 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：標準

一般社員は顧客情報を閲覧だけでき、管理者だけが更新できるようにする考え方はどれか。

ア. 全利用者へ管理者権限を与える。

イ. 利用者や役割に応じてアクセス権を設定する。

ウ. 誰でも匿名で更新できるようにする。

エ. アクセス権を設定せず、注意書きだけで運用する。

解答・解説 正答：イ

ア：必要以上の権限付与となります。

イ：必要な利用者に必要な権限だけを与えるアクセス制御が基本です。

ウ：情報の完全性や機密性を損なう恐れがあります。

エ：技術的な制御が不足します。

総合解説：アクセス制御では、最小権限の考え方に基づき必要な権限だけを付与します。

問題 0147 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：標準

デジタル証明書と認証局を利用し、公開鍵の持ち主が誰であるかを信頼できる形で確認するための基盤はどれか。

ア. VPN

イ. SIEM

ウ. PKI

エ. DLP

解答・解説 正答：ウ

ア：通信路を保護する仕組みです。

イ：ログの集約・分析を行う仕組みです。

ウ：PKIはPublic Key Infrastructureで、公開鍵と本人・組織の対応を証明書で管理します。

エ：情報漏えい防止に利用される仕組みです。

総合解説：PKIでは認証局、デジタル証明書、ルート証明書などを用いて公開鍵への信頼を構築します。

問題 0148 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：応用

公開鍵と証明書の申請者との対応を確認し、デジタル証明書を発行・管理する機関はどれか。

ア. CSIRT

イ. SOC

ウ. ISP

エ. CA（認証局）

解答・解説 正答：エ

ア：セキュリティインシデントへの対応組織です。

イ：セキュリティ監視・分析を行う組織です。

ウ：インターネット接続サービスを提供する事業者です。

エ：CAはCertification Authorityで、デジタル証明書の発行や管理を行います。

総合解説：PKIではCAが証明書を発行し、公開鍵とその所有者との対応を信頼できる形で示します。

問題 0149 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：応用

有効期限内でも、秘密鍵漏えいなどの理由で無効になったデジタル証明書を確認するための一覧はどれか。

ア. CRL

イ. ACL

ウ. URL

エ. RPO

解答・解説

正答：ア

ア：CRLはCertificate Revocation Listで、失効した証明書の情報を確認するために利用されます。

イ：アクセス権を定義するアクセス制御リストです。

ウ：Web資源の場所を表すものです。

エ：データ復旧時点の目標です。

総合解説：デジタル証明書は有効期限だけでなく、失効していないかを確認することも重要です。

問題 0150 [6-5 セキュリティ対策] > [認証・アクセス制御・PKI] ｜ 難易度：応用

重要な社内システムで、本人確認を強化し、ログイン後も担当業務に必要な機能だけ利用させたい。最も適切な組合せはどれか。

ア. 認証だけ行い、全利用者へ全権限を与える。

イ. 多要素認証で本人確認を強化し、役割に応じたアクセス制御で利用可能な機能を制限する。

ウ. アクセス制御だけ行い、本人確認を行わない。

エ. 暗号化だけ行い、認証も権限管理も行わない。

解答・解説

正答：イ

ア：ログイン後の権限管理が不十分です。

イ：認証は『誰か』を確認し、アクセス制御は『何をしてよいか』を決めるため、両方が必要です。

ウ：他人によるなりすましを防ぎにくくなります。

エ：利用者と操作権限を適切に管理できません。

総合解説：セキュリティでは、認証、認可・アクセス制御、監査ログなど複数の仕組みを組み合わせます。