問 1 正解 完璧 直前チェック

ITサービスマネジメントにおけるインシデント及びサービス要求管理プロセスと問題管理プロセスとのインタフェースに関する要件のうち，適切なものはどれか。

ア　インシデント及びサービス要求管理プロセスでは，インシデント解決の進捗状況を問題管理プロセスに伝えなければならない。
イ　インシデント及びサービス要求管理プロセスでは，インシデントの根本原因を調査して，その結果を問題管理プロセスに伝えなければならない。
ウ　問題管理プロセスでは，既知の誤り及び問題解決策に関する最新の情報を，インシデント及びサービス要求管理プロセスに提供しなければならない。
エ　問題管理プロセスでは，問題の根本原因を正すために要求される変更を，インシデント及びサービス要求管理プロセスに伝えなければならない。

問 2 正解 完璧 直前チェック

JIS Q 20000-1において，サービスレベル管理は，サービスマネジメントシステム(SMS)を構成するどのプロセスに属するか。

ア　解決プロセス　　イ　関係プロセス
ウ　サービス提供プロセス　　エ　統合的制御プロセス

問1　ウ

解説

ITサービスマネジメントにおける**インシデント及びサービス要求管理プロセス**：ITサービスマネジメントの「解決プロセス」は，障害発生や顧客からの要望に対して，復旧や解決を提供する。そのうち「インシデント及びサービス要求管理」は顧客対応を中心とした処置を，「問題管理」はサービス提供者がインシデントの根本原因の解決を図るものである。

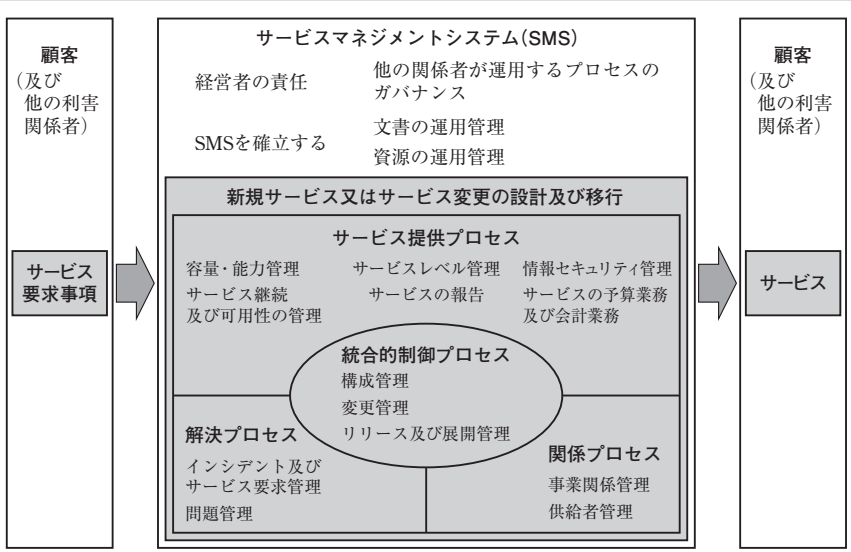
問題管理プロセス：発生した不具合，あるいは今後起きるかもしれない不具合の根本原因を追究するプロセス。目標はサービスが安定し，問題が再発しないことを確認することにある。

ア：インシデントの追跡とライフサイクルの管理は，インシデント管理プロセスで行う。
イ：インシデントの根本原因の調査は，問題管理プロセスで行う。
エ：問題の根本原因を正すための変更の管理は，変更管理プロセスで行う。

問2　ウ

解説　**JIS Q 20000-1**：サービスマネジメントシステム要求事項。ITサービスを提供する組織のITサービスマネジメント(ITSM)が適切であるかどうかを評価するための認証基準およびガイドラインである。

下図にあるように，サービスレベル管理はサービス提供プロセスに属する。



出典：「JIS Q 20000-1：2012 図2 -サービスマネジメントシステム(SMS)」より

問 3 正解 完璧 直前チェック

ITILにおいて，良い目標値を設定するための条件として“SMART”がある。“S”はSpecific（具体的），“M”はMeasurable（測定可能），“R”はRelevant（適切），“T”はTime-bound（適時）の頭文字である。“A”は何の頭文字か。

ア　Achievable（達成可能）　　イ　Ambitious（意欲的）
ウ　Analyzable（分析可能）　　エ　Auditable（監査可能）

問 4 正解 完璧 直前チェック

“ITサービスが必要とされるときに，合意した条件の下で要求された機能を果たせる状態にある能力”について，定義し，分析し，計画し，測定し，改善する活動を行うITILの管理プロセスはどれか。

ア　ITサービス継続性管理　　イ　インシデント管理
ウ　可用性管理　　エ　問題管理

問 5 正解 完璧 直前チェック

サービスレベル管理における運用レベル合意書（OLA）はどれか。

ア　SLAを実現するために，サービス提供者が同じ組織内の内部グループとの間で取り交わす合意書
イ　SLAを実現するために，サービス提供者が供給者との間で取り交わす契約書
ウ　サービス提供者が顧客に提出する，SLAの達成状況や未達成事項をまとめた文書
エ　サービスレベルに関して，サービス提供者が顧客との間で取り交わす合意書

問3　ア

解説　ITILにおいて，良い目標値を設定するための条件“SMART”は，サービスレベル・アグリーメントおよびプロジェクト計画における目標値が，具体的（Specific），測定可能（Measurable），達成可能（Achievable），適切（Relevant），および適時（Timely）であるべきということを覚えやすくするための頭字語である。

問4　ウ

解説

IT サービス継続性管理：災害などでシステムが停止した場合，最小限の業務要件をサポートするために実施する管理プロセス。インシデント管理との違いは，事業要件に合わせて最低限の復旧を行う点である。

インシデント管理：できる限り早く利用者が通常の利用状況へ戻れるように対応する活動。対応策が既にわかっている場合や，根本的な原因がわからない状況であっても，すぐに復旧させることを優先させる。

可用性管理：IT サービスを顧客が利用しようとしたときに，サービスが継続して利用できるようになっていること。

問題管理：未知の問題が発生したときに，その問題を回避するための方策を立案すること。原因の調査，復旧対策の検討や恒久対策の実施である。

問5　ア

解説　**運用レベル合意書**（OLA：Operational Level Agreement）：ITサービス提供者の内部で結ばれる文書。クライアントに対するITサービスのサポートおよびデリバリに関する責任範囲，障害発生時の活動などを定義する。

イ：**外部委託契約**（UC：Underpinning Contract）の説明。

ウ：**サービス報告書**（Service Report）の説明。

エ：**サービスレベル合意書**（SLA：Service Level Agreement）の説明。

問 6 正解 完璧 直前チェック

ITサービスマネジメントにおいて，災害による重大なサービス停止に関する事業影響度分析は，どのプロセスで実施するか。

ア　インシデント及びサービス要求管理
イ　サービス継続及び可用性管理
ウ　サービスレベル管理
エ　問題管理

問 7 正解 完璧 直前チェック

ITサービスマネジメントにおける変更要求に対する活動のうち，リリース及び展開管理プロセスに含まれるものはどれか。

ア　稼働環境に展開される変更された構成品目（CI）の集合の構築
イ　変更の影響を受ける構成品目（CI）の識別
ウ　変更要求（RFC）の記録
エ　変更要求を評価するための変更諮問委員会（CAB）の召集

問 8 正解 完璧 直前チェック

ITサービスマネジメントにおいて，構成ベースラインを確立することによって可能になることはどれか。

ア　ITサービスの存続期間を通したパフォーマンスの変化の測定
イ　インシデントが発生したときの問題管理プロセスでの状況証拠の分析
ウ　構成監査及び切り戻しのための基準の提供
エ　サービスを機能させるために必要な最低限の利用可能レベルの定義

問6　イ

解説

インシデント及びサービス要求管理：顧客からの要求を解決するための運用管理プロセス。

サービス継続及び可用性管理：サービス継続管理は，提供するITサービスが中断した場合に備えて，全ての技術要素や設備，機能を合意された期間内に再開できるように事前対策を講じるプロセス。可用性管理は，SLAで合意されたITサービスをコストの最適化を図りながら確実に実施，維持する仕組みを構築するプロセス。

サービスレベル管理：ITサービスにおいて，顧客と合意したサービスレベルの提供，維持，改善するために管理するプロセス。

問題管理：インシデント及び問題がビジネスに対して与える悪影響を最小限に留め，インシデントの再発を防ぐためのプロセス。

問7　ア

解説　**リリース及び展開管理プロセス**：リリース管理と展開の両方を責務とするプロセス。リリース計画・手順を策定し，その実行が確実に行われることをコントロールする。

イ：構成管理プロセスに含まれる。

ウ，エ：変更管理プロセスに含まれる。

問8　ウ

解説　**構成ベースライン**：ITIL における構成ベースラインとは，正式に合意済みで，変更管理プロセスを通して管理される構成のベースラインを意味する。構成ベースラインは，将来の構成，リリース，および変更のベースとして使用する。

ア：サービス測定基準を確立することで可能になる。

イ：インシデント発生時にスナップショットを保存することで可能になる。

エ：サービスレベル管理を行うことで可能になる。

問 9 正解 完璧 直前チェック

ITILにおいて，インシデントに対する一連の活動のうち，イベント管理プロセスが分担する活動はどれか。

ア　インシデントの発生後に，インシデントの原因などをエラーレコードとして記録する。
イ　インシデントの発生後に，問題の根本原因を分析して記録する。
ウ　インシデントの発生時に，ITサービスを迅速に復旧するための対策を講じる。
エ　インシデントの発生を検出して，関連するプロセスに通知する。

問 10 正解 完璧 直前チェック

ITILで定義されるサービスのライフサイクルにおけるサービストランジション段階の説明はどれか。

ア　規定された要件と制約に沿って，サービスを運用に移行し，確実に稼働させることである。
イ　サービスの効率，有効性，費用対効果の観点で運用状況を継続的に測定し，改善していくことである。
ウ　サービスの内容を具体的に決めることである。
エ　戦略的資産として，どのようにサービスマネジメントを設計，開発，導入するかについての手引を提供することである。

問 11 正解 完璧 直前チェック

バックアップサイトの説明のうち，ウォームスタンバイの説明として，最も適切なものはどれか。

ア　同じようなシステムを運用する外部の企業や組織と協定を結び，緊急時には互いのシステムを貸し借りして，サービスを復旧する。
イ　緊急時にバックアップシステムを持ち込んでシステムを再開し，サービスを復旧する。
ウ　別の場所に常にデータの同期が取れているバックアップシステムを用意しておき，緊急時にバックアップシステムに切り換えて直ちにサービスを復旧する。
エ　別の場所にバックアップシステムを用意しておき，緊急時にバックアップシステムを起動してデータを最新状態にする処理を行った後にサービスを復旧する。

問9　エ

解説　**イベント管理プロセス**：全てのIT インフラから発生するイベントを監視し，運用が通常通りに行われていることを確認する。異常なイベントが検知された際には，インシデント管理など他の管理プロセスへエスカレーションする。
ア，ウ：**インシデント管理**の説明である。
イ：**問題管理**の説明である。

問10　ア

解説　**サービストランジション段階**：ITサービスやその他の構成アイテムが，ライフサイクル中のあるステータスから次のステータスに移ることに応じた状態変移の活動またはプロセス。
イ：**継続的サービス改善**の説明である。
ウ：**サービスデザイン**の説明である。
エ：**サービスストラテジ**の説明である。

問11　エ

解説
バックアップサイト：予備のコンピュータセンタのこと。大規模な自然災害などにより主系のコンピュータセンタのシステムが利用できなくなったときに切り換えて事業継続のために利用する。
ウォームスタンバイ：2系統のシステムを用意しておき，一方を主系として常用し，もう一方は電源を入れてOSなどを起動して待機系とするスタンバイ方式。主系に障害が発生すると待機系でシステムを立ち上げ，データを最新状態にする処理を行った上でシステムを切り換える。待機系と常に同期を取るホットスタンバイと，待機系は動作させないでおくコールドスタンバイの中間の方式である。
ア：**BCP対策**の一例の説明である。
イ：**コールドスタンバイ**の説明である。
ウ：**ホットスタンバイ**の説明である。

問 12 正解 完璧 直前チェック

データベースのロールバック処理の説明はどれか。

ア　ログの更新後情報を用いて，トランザクション開始後の障害直前の状態にまでデータを復元させる。
イ　ログの更新後情報を用いて，トランザクション開始直前の状態にまでデータを復元させる。
ウ　ログの更新前情報を用いて，トランザクション開始後の障害直前の状態にまでデータを復元させる。
エ　ログの更新前情報を用いて，トランザクション開始直前の状態にまでデータを復元させる。

問 13 正解 完璧 直前チェック

“24時間365日”の有人オペレーションサービスを提供する。シフト勤務の条件が次のとき，オペレータは最少で何人必要か。

〔条件〕
(1)　1日に3シフトの交代勤務とする。
(2)　各シフトで勤務するオペレータは2人以上とする。
(3)　各オペレータの勤務回数は7日間当たり5回以内とする。

ア　8　　イ　9　　ウ　10　　エ　16

問 14 正解 完璧 直前チェック

情報セキュリティに関する従業員の責任について，“情報セキュリティ管理基準”に基づいて監査を行った。指摘事項に該当するものはどれか。

ア　雇用の終了をもって守秘責任が解消されることが，雇用契約に定められている。
イ　定められた勤務時間以外においても守秘責任を負うことが，雇用契約に定められている。
ウ　定められた守秘責任を果たさなかった場合，相応の措置がとられることが，雇用契約に定められている。
エ　定められた内容の守秘義務契約書に署名することが，雇用契約に定められている。

問12　エ

解説　**ロールバック**：トランザクションの途中，プログラムのバグなどでアプリケーションからの応答がなくなったり，強制終了したりした場合に，ログの更新前情報（更新前ジャーナル）を用いてデータベースをトランザクション開始直前の状態に戻す処理のこと。

問13　イ

解説　シフト勤務の条件から必要なオペレータの人員数を計算する。
(1) より1日当たり3シフト勤務
(2) より1シフトに勤務するオペレータは2人以上なので，3シフト×2人＝6シフト/日
(3) より1人の勤務回数は，7日間×3シフト×2人＝42シフト中の5回以内
7日間当たりのシフト勤務の条件が365日続くと考えてよいから，42÷5＝8.4
オペレータは最少で9人以上必要である。

問14　ア

解説　**情報セキュリティ管理基準**：経済産業省の情報セキュリティ管理基準（平成20年改正版）は，マネジメント基準と管理策基準から構成される。

マネジメント基準では，情報セキュリティマネジメントの計画，実行，点検，処置に必要な実施事項を定めている。マネジメント基準のそれぞれの事項は，JIS Q 27001:2006をもとにして策定されている。

管理策基準は，組織に情報セキュリティマネジメントの確立段階において，リスク対応方針に従って管理策を選択する際の選択肢を与えるものである。管理策基準のそれぞれの事項は，JIS Q 27001:2006附属書A「管理目的及び管理策」，JIS Q 27002:2006をもとに専門家の知見を加えて作成され，管理目的と管理策で構成される。

ア：情報セキュリティ管理基準の管理策基準「4人的資源のセキュリティ」の「4.3雇用の終了又は変更」に「雇用終了後もなお有効な責任及び義務を，従業員，契約相手及び第三者の利用者の契約に含める」と明記されているため，守秘責任の解消をしている点が指摘事項になる。

問 15 正解 □ 完璧 □ 直前チェック □

データ管理者（DA）とデータベース管理者（DBA）を別々に任命した場合のDAの役割として，適切なものはどれか。

ア　業務データ量の増加傾向を把握し，ディスク装置の増設などを計画して実施する。
イ　システム開発の設計工程では，主に論理データベース設計を行い，データ項目を管理して標準化する。
ウ　システム開発のテスト工程では，主にパフォーマンスチューニングを担当する。
エ　システム障害が発生した場合には，データの復旧や整合性のチェックなどを行う。

問15　イ

解説

データ管理者（DA）：業務の実世界から概念設計を行い，システム化の範囲で論理設計を行う。

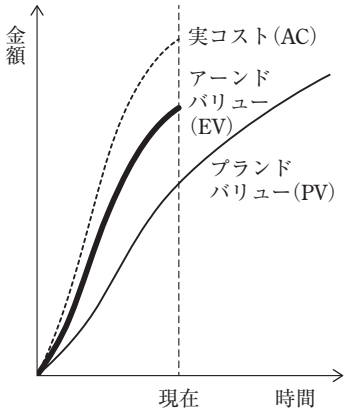
データベース管理者（DBA）：論理データモデルから物理設計を行い，データベースを構築する。また，構築後のデータベースの運用設計および運用保守等も行う。

ア，ウ，エ：データベース管理者（DBA）の役割である。

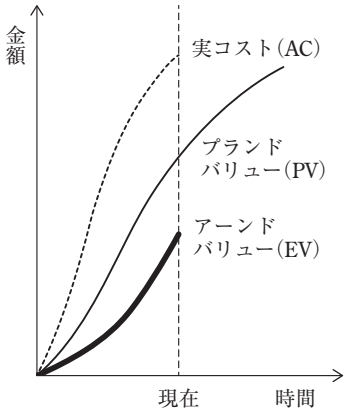
問 16 正解 □ 完璧 □ 直前チェック □

プロジェクトの進捗管理をEVM（Earned Value Management）で行っている。コストが超過せず，納期にも遅れないと予想されるプロジェクトはどれか。ここで，それぞれのプロジェクトの開発の生産性は現在までと変わらないものとする。

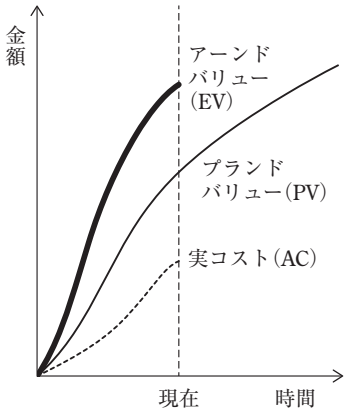
ア



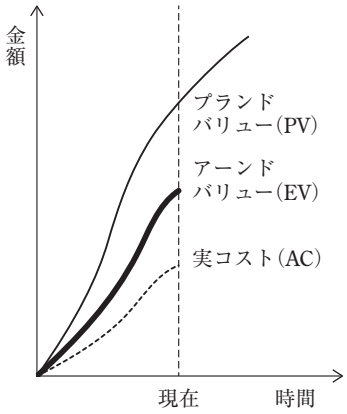
イ



ウ



エ



問16 ウ

解説

EVM：作業の進捗や達成度の金銭的表現（Earned Value）を統一的な尺度として，プロジェクトのパフォーマンス（コスト，スケジュール）を定量的に測定・分析し，一元的な管理を行うプロジェクト管理手法。

プランドバリュー（PV）：成果物の作成期限と必要な金額を見積もること。

アーンドバリュー（EV）：現在の出来高を示し，成果物の完成状況を確認すること。

実コスト（AC）：実際に必要となった費用。PVと比較することで，予算に対する実績がわかる。

図中の現在の時点でコストが超過していないプロジェクトはPVよりもACが下回っていて，納期にも遅れていないと予想されるということは，EVがPVを上回っているものであるから選択肢ウが正解である。

問 17 正解 完璧 直前チェック

プロジェクト管理で使用する分析技法のうち，傾向分析の説明はどれか。

ア　個々の選択肢とそれぞれを選択した場合に想定されるシナリオの関係を図に表し，それぞれのシナリオにおける期待値を計算して，最善の策を選択する。
イ　個々のリスクが現実のものとなったときの，プロジェクトの目標に与える影響の度合いを調べる。
ウ　時間の経過に伴うプロジェクトのパフォーマンスの変動を検討する。
エ　発生した障害とその要因の関係を魚の骨のような図にして分析する。

問 18 正解 完璧 直前チェック

プロジェクトのリスクを，デルファイ法を利用して抽出しているものはどれか。

ア　ステークホルダや経験豊富なプロジェクトマネージャといった専門家にインタビューし，回答を収集してリスクとしてまとめる。
イ　複数のお互いに関係のないステークホルダやプロジェクトマネージャにアンケートを行い，その結果を要約する。さらに，要約結果を用いてアンケートを行い，結果を要約することを繰り返してリスクをまとめる。
ウ　プロジェクトチームのメンバにPMOのメンバやステークホルダを複数名加え，一堂に会して会議をし，リスクに対する意見を出し合い，進行役がリスクとしてまとめる。
エ　プロジェクトを強み，弱み，好機，脅威のそれぞれの観点及びその組合せで分析し，リスクをまとめる。

問17　ウ

解説　**傾向分析**：時間の経過と共にパフォーマンスが改善しているか悪化しているかを判断するためにパフォーマンスの変動を検討する分析技法。
ア：**What-if分析**の説明である。
イ：**プロジェクト・リスクマネジメント**の説明である。
エ：**魚骨図**（フィッシュボーンチャート）を用いた分析手法の説明。

問18　イ

解説　**デルファイ法**：技術予測やその未来を予測したいテーマに対して，複数の専門家や有識者にアンケートを繰り返し行い，客観性を与えながら意見を集約・洗練させて，角度の高い結論を求める方法である。
ア：**インタビュー法**の説明である。
ウ：**ブレイン・ストーミング**の説明である。
エ：**SWOT**（Strength Weakness Opportunity Threat）**分析**の説明である。

問 19 正解 □ 完璧 □ 直前チェック □

パイプラインハザード対策に関する記述のうち，アウトオブオーダ実行方式を用いたものはどれか。

ア　演算に必要なデータがそろうまで実行が待たされている命令によって，後続の命令の実行が待たされることを防ぐために，既にデータがそろっている後続の命令があれば，それを先に実行する。

イ　条件分岐命令の判定結果が分かるまで分岐後の命令実行が待たされることを防ぐために，分岐する確率が高い方の命令を先読みして実行する。

ウ　前の命令の演算結果がレジスタに書き込まれるまで次の命令の実行が待たされることを防ぐために，プロセッサ内にバイパス経路を設け，演算結果を演算器に直接入力して次の命令を実行する。

エ　レジスタへのアクセスが競合して後続の命令の実行が待たされることを防ぐために，クロックサイクルを細分化し，サイクル前半を書込み，後半を読出しとすることで競合なく命令を実行する。

問 20 正解 □ 完璧 □ 直前チェック □

二つのシステムの信頼性評価指標の関係に関する記述のうち，適切なものはどれか。

ア　稼働率が等しければ，MTBFも等しい。

イ　稼働率が等しければ，MTTRも等しい。

ウ　故障発生率が等しければ，MTBFも等しい。

エ　故障発生率が等しければ，MTTRも等しい。

春 秋

問19　ア

解説

パイプラインハザード対策：パイプライン制御を行っていても，命令の依存関係などの理由で先読み処理がうまく機能せず，命令の並列処理が中断してしまう状態を**パイプラインハザード**という。

アウトオブオーダ実行方式：命令を一時的に溜め，命令を細分化して，できる作業から実行する方式。プロセッサが命令を処理するときに規定の順番を守らないやり方。

ちなみに，旧来のプロセッサでは命令を読み込む，命令が実行ユニットに移される，命令ユニットで実行する，結果を返す，という手順（**インオーダー実行方式**）で忠実に実行されており，実行に必要なデータがそろうまでの待ち時間を生じていた。

問20　ウ

解説　システムの信頼性評価指標の関係は次のとおりである。

稼働率：システムが正常に動いている時間の割合。

稼働率 = MTBF/(MTBF + MTTR)

故障発生率：単位時間内でどの程度故障するかの割合（確率）。

故障率発生 = 1/MTBF

MTBF（Mean Time Between Failure）：平均故障間隔。故障するまでの時間の平均値。

MTBF = 製品の稼働時間/故障件数

MTTR（Mean Time To Repair）：平均故障修理時間。修理にかかった時間の平均値。

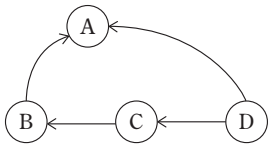
MTTR = 製品の修理時間合計/故障回数

故障発生率が等しければMTBFも等しい。

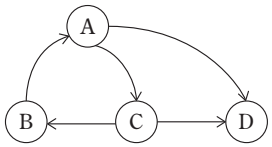
問 21 正解 完璧 直前チェック

トランザクションA～Dに関する待ちグラフのうち，デッドロックが発生しているものはどれか。ここで，待ちグラフの矢印は，$X \rightarrow Y$のとき，トランザクションXはトランザクションYがロックしている資源のアンロックを待っていることを表す。

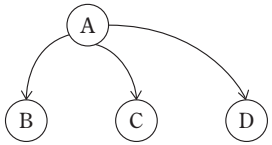
ア



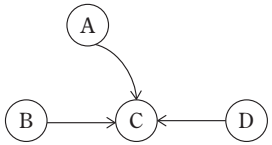
イ



ウ

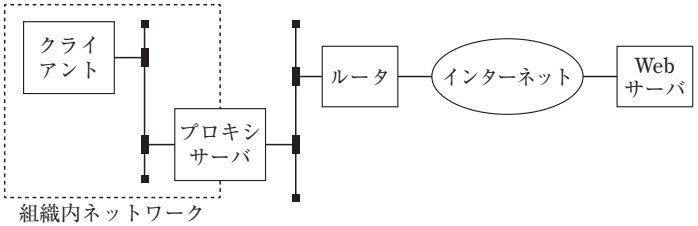


エ



問 22 正解 完璧 直前チェック

図は，組織内のTCP/IPネットワークにあるクライアントが，プロキシサーバ，ルータ，インターネットを経由して組織外のWebサーバを利用するときの経路を示している。この通信のTCPコネクションが設定される場所はどれか。



ア　クライアントとWebサーバの間，クライアントとプロキシサーバの間
イ　クライアントとプロキシサーバの間，プロキシサーバとWebサーバの間
ウ　クライアントとプロキシサーバの間，プロキシサーバとルータの間，ルータとWebサーバの間
エ　クライアントとルータの間，ルータとWebサーバの間

問21　イ

解説

待ちグラフ：どのトランザクションが，どのトランザクションのアンロックを待っているかグラフに示したもの。待ちグラフにサイクル（閉路）ができるとデットロック状態である。

デッドロック：複数のトランザクションが互いのアンロックを延々と待ち続け一切処理が進まない状態のこと。

問22　イ

解説　プロキシサーバは，クライアントが組織内のネットワークにあって，目的のWebサーバと直接接続できないときに使用する中継サーバである。クライアントはプロキシサーバのみにTCPコネクションを設定し，プロキシサーバはWebサーバのみにTCPコネクションを設定する。ルータはOSI第3層のネットワーク層で中継するため，TCPコネクション（第4層：トランスポート層）の設定は行わない。

ア：クライアントと組織外のWebサーバ間のTCPコネクションが設定されているところが誤り。

ウ，エ：ルータはIP層でパケットを中継するので，TCPコネクションは設定されない。

問 23 正解 完璧 直前チェック

シングルサインオンの実装方式の特徴のうち，適切なものはどれか。

ア　クッキーを使ったシングルサインオンの場合，サーバごとの認証情報を含んだクッキーをクライアントで生成し，各サーバ上で保存，管理する。
イ　クッキーを使ったシングルサインオンの場合，認証対象のサーバを，異なるインターネットドメインに配置する必要がある。
ウ　リバースプロキシを使ったシングルサインオンの場合，認証対象のWebサーバを，異なるインターネットドメインに配置する必要がある。
エ　リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。

問 24 正解 完璧 直前チェック

NISTの定義によるクラウドコンピューティングのサービスモデルにおいて，パブリッククラウドサービスの利用企業のシステム管理者が，仮想サーバのゲストOSに関わる設定作業及びセキュリティパッチ管理作業を実施可かどうかの組合せのうち，適切なものはどれか。

	IaaS	PaaS	SaaS
ア	実施可	実施可	実施不可
イ	実施可	実施不可	実施不可
ウ	実施不可	実施可	実施不可
エ	実施不可	実施不可	実施可

問 25 正解 完璧 直前チェック

刑法の電子計算機使用詐欺罪が適用される違法行為はどれか。

ア　いわゆるねずみ講方式による取引形態のWebページを開設する。
イ　インターネット上に，実際よりも良品と誤解される商品カタログを掲載し，粗悪な商品を販売する。
ウ　インターネットを経由して銀行のシステムに虚偽の情報を与え，不正な振込や送金をさせる。
エ　企業のWebページを不正な手段で改変し，その企業の信用を傷つける情報を流す。

春
秋

問23　エ

解説　**シングルサインオン**：一度の認証手続きで複数のサーバにアクセスできる仕組み。
ア：クッキーはクライアント上で保存，管理する。
イ：認証対象のサーバを，同一インターネットドメインに配置する必要がある。
ウ：認証対象のWebサーバを，同一インターネットドメインに配置する必要がある。

問24　イ

解説
クラウドコンピューティング：コンピュータ資源をインターネットなどのネットワークを通じてサービスの形で利用する方式のこと。
IaaS（Infrastructure as a Service）：サーバ，CPU，ストレージなどのインフラをサービスとして提供する。仮想サーバのゲストOSを直接操作できるため，設定作業やセキュリティパッチ管理作業が実施可能である。
PaaS（Platform as a Service）：ソフトウェアを稼働させるプラットフォーム（基盤）をサービスとして提供する。仮想サーバのゲストOSを直接操作できないため，設定作業やセキュリティパッチ管理作業は実施不可能である。
SaaS（Software as a Service）：ソフトウェアをサービスとして提供する。仮想サーバのゲストOSを直接操作できないため，設定作業やセキュリティパッチ管理作業は実施不可能である。

問25　ウ

解説　**電子計算機使用詐欺罪**：コンピュータを操作して他人をだまし，不実の電磁的記録を作るなどの手段により，財産上の利益を得る犯罪。
ア：**無限連鎖防止法**（ねずみ講防止法）が適用される。
イ：**詐欺罪**が適用される。
エ：**電子計算機損壊等業務妨害**が適用される。