

平成 17 年度 春期

テクニカルエンジニア（システム管理） 午前 問題

注意事項

1. 試験開始の合図があるまで、問題冊子を開いて中を見てはいけません。
2. この注意事項は、問題冊子の裏表紙にも続きます。問題冊子を裏返して必ず読んでください。
3. 答案用紙への受験番号などの記入及びマークは、試験開始の合図があってから始めてください。
4. 試験時間は、次の表のとおりです。

試験時間	9:30 ～ 11:10（1 時間 40 分）
------	-------------------------

途中で退出する場合には、手を挙げて監督員に合図し、答案用紙が回収されてから静かに退出してください。

退出可能時間	10:30 ～ 11:00
--------	---------------

5. 問題は、次の表に従って解答してください。

問題番号	問 1 ～ 問55
選択方法	全問必須

6. 問題に関する質問にはお答えできません。文意どおり解釈してください。
7. 問題冊子の余白などは、適宜利用して構いませんが、どのページも切り離さないでください。
8. 電卓は、使用できません。

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して、必ず読んでください。

問1 キャッシュメモリのアクセス時間が主記憶のアクセス時間の $1/30$ で、ヒット率が 95% のとき、主記憶の実効アクセス時間は、主記憶のアクセス時間の約何倍になるか。

ア 0.03 イ 0.08 ウ 0.5 エ 0.95

問2 ディスプレイの解像度が 800×600 画素のとき、最大 2^{16} 色の色数で表示できるパソコンがある。解像度を $1,600 \times 1,200$ 画素にしたとき、表示できる最大の色数は幾らか。ここで、主記憶の一部をビデオメモリとして使用することはないものとする。

ア 2^4 イ 2^8 ウ 2^{12} エ 2^{16}

問3 OS のプロセス制御におけるプリエンプティブ方式に関する記述として、適切なものはどれか。

ア 各プロセスがシステム資源を自主管理できるので、マルチプログラミングに向いている。

イ ノンプリエンプティブ方式に比べて、コンテキスト切替えのためのオーバーヘッドが小さい。

ウ ノンプリエンプティブ方式に比べて、特定のプロセスがプロセッサを独占することが多い。

エ プリエンプティブ方式を実現するには、OS がプロセスを強制的に切り替えて実行する機構が必要になる。

問4 仮想記憶方式において、仮想アドレスと物理アドレスとを対応付けるアドレス変換機能に付加情報を与えることで、実現が容易になるものはどれか。

- | | |
|-------------|--------------|
| ア オーバレイ | イ 記憶保護 |
| ウ メモリインタリーブ | エ メモリコンパクション |

問5 2 階層型のクライアントサーバ方式の業務システムを、ストアードプロシージャを使って書き直す場合、最も期待できる効果はどれか。

- ア クライアントとサーバ間の通信回数が減少する。
- イ サーバの CPU 負荷が減少する。
- ウ サーバのディスクアクセスの回数が減少する。
- エ データベースへの、より複雑なアクセスが可能となる。

問6 1 台のプリンタを複数台のパソコンで共有するシステムがある。このプリンタに対する平均要求回数が毎分 1 回のとき、このプリンタの平均応答時間（印刷を要求してから終了するまでの時間）は何秒か。ここで、プリンタは、平均が 15 秒の指数分布に従う印刷時間で要求を処理するものとし、プリンタに対する要求はポアソン分布に従うものとする。

- | | | | |
|------|------|------|------|
| ア 15 | イ 18 | ウ 20 | エ 30 |
|------|------|------|------|

問 7 1 件のデータについて，読取りに 40 ミリ秒，CPU 処理に 30 ミリ秒，書込みに 50 ミリ秒かかるプログラムがある。このプログラムで， n 件目の書込みに併せて $n+1$ 件目の CPU 処理と $n+2$ 件目の読取りを並行して行くと，1 分当たりの最大データ処理件数は幾つか。ここで，OS のオーバヘッドは考慮しないものとする。

ア 500

イ 666

ウ 750

エ 1,200

問 8 客観的な性能評価を行う目的で設定された指標又はベンチマークのうち，端末，ネットワーク，ソフトウェアなども含んだ，システム全体としての性能を評価するものはどれか。

ア Dhrystone/MIPS

イ Linpack

ウ SPECint/SPECfp

エ TPC-C

問 9 コンピュータシステムにおいて，改善手法を適用した機能部分の全体に対する割合を R ($0 < R < 1$)，その部分の改善手法を適用する前に対する適用した後の性能比を A とする。このとき，全体の性能比を表す式はどれか。

ア $\frac{1}{(1-R) \times A}$

イ $\frac{1}{(1-R) + \frac{R}{A}}$

ウ $\frac{1}{R + \frac{1-R}{A}}$

エ $\frac{1}{\frac{R}{A}}$

問10 キャパシティプランニングにおけるサービス管理の説明のうち、適切なものはどれか。

- ア 単位時間に処理可能な作業量を見積もって、ハードウェア構成や機器を選択する。
- イ 提供するサービスの水準を達成するのに必要な経費を管理する。
- ウ ハードウェア構成や機器の処理速度を決定するために、業務負荷の特性及び組成要素を明らかにする。
- エ ユーザ部門が期待するパフォーマンスと提供されるサービスのコストを、責任分担を明らかにして管理する。

問11 1 台のサーバと 3 台のクライアントが接続されたシステムがある。システムを利用するためには、サーバと少なくともいずれか 1 台のクライアントが稼働していればよい。サーバの稼働していない確率を a 、各クライアントの稼働していない確率をいずれも b とすると、このシステムが利用できない確率を表す式はどれか。

- ア $1-(1-a)(1-b^3)$
- イ $1-(1-a)(1-b)^3$
- ウ $(1-a)(1-b)^3$
- エ $1-ab^3$

問12 東京～大阪及び東京～名古屋がそれぞれ独立した通信回線で接続されている。東京～大阪の稼働率は 0.9、東京～名古屋の稼働率は 0.8 である。東京～大阪の稼働率を 0.95 以上に改善するために、大阪～名古屋にバックアップ回線を新設することを計画している。新設される回線の稼働率は最低限幾ら必要か。

- ア 0.167
- イ 0.205
- ウ 0.559
- エ 0.625

問13 三つの装置 A ～ C で構成されるシステムがある。三つの装置すべてが正常に稼働しないとシステムは機能しない。各装置の MTBF は表のとおりである。システム全体の MTBF は何時間か。

装置	MTBF (時間)
A	600
B	900
C	1,800

ア 300 イ 600 ウ 900 エ 1,100

問14 データマイニングに関する説明として、適切なものはどれか。

- ア 基幹業務のデータベースとは別に作成され、更新処理をしない時系列データの分析を主目的とする。
- イ 個人別データ、部門別データ、サマリデータなど、分析者の目的別に切り出され、カスタマイズされたデータを分析する。
- ウ スライシング、ダイシング、ドリルダウンなどのインタラクティブな操作によって多次元分析を行い、意思決定を支援する。
- エ ニューラルネットワークや統計解析などの手法を使って、大量に蓄積されているデータから、顧客購買行動の法則などを探し出す。

問15 システムを構成する要素のうち、次の特徴をもつものはどれか。

- (1) 利用者から仕事を託され、ネットワーク内でその仕事を処理するのに必要な場所（サーバ）を自律的に巡って、仕事を片付ける。
- (2) すべての仕事が終了した時点で利用者の下に戻る。
- (3) ネットワーク内に送出された後、返ってくるまで、利用者はネットワークにアクセスする必要はない。

ア エージェント

イ クライアント

ウ スクリプト

エ プロセス

問16 CMM に関する記述として、適切なものはどれか。

- ア 各種のソフトウェア設計・開発技法を使って開発作業を自動化し、ソフトウェア開発の生産性向上を図る。
- イ ソフトウェアライフサイクルを、主プロセス、支援プロセス、組織プロセスの三つに分けて作業内容を定め、ソフトウェアプロセスの標準化を図る。
- ウ ソフトウェアを開発する組織のプロセス成熟度モデルを使って、プロセスの改善を図る。
- エ 特定の購入者と製作者の間で授受されるソフトウェア製品の品質保証を行う。

問17 モジュールの独立性を高めるには、モジュール結合度を弱くする必要がある。モジュール間の情報の受渡し方法のうち、モジュール結合度が最も弱いものはどれか。

- ア 共通域に定義したデータを、関係するモジュールが参照する。
- イ 制御パラメタを引数として渡し、モジュールの実行順序を制御する。
- ウ データ項目だけをモジュール間の引数として渡す。
- エ 必要なデータだけを外部宣言して共有する。

問18 次のテストケース設計法を何と呼ぶか。

読み込んだデータが正しくないとき，エラーメッセージを出力するかどうかをテストしたい。プログラム仕様書を基に，正しくないデータのクラスを識別し，その中から任意の一つのデータを代表として選んでテストケースとした。

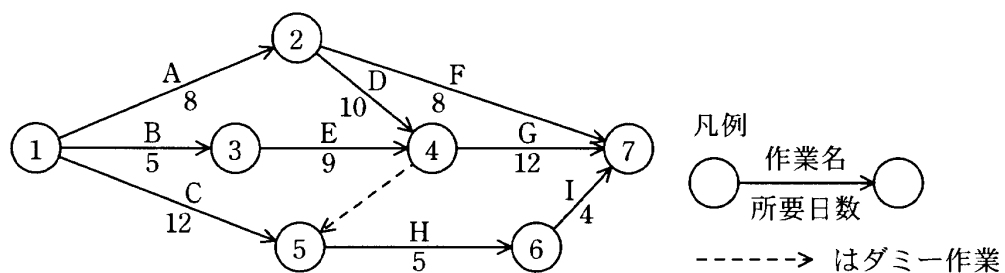
ア 原因結果グラフ

イ 限界値分析

ウ 同値分割

エ 分岐網羅

問19 あるプロジェクトの作業が図に従って計画されているとき，最短日数で終了するために結合点⑤を通過していなければいけないのは，プロジェクトの開始から遅くとも何日後か。



ア 12

イ 14

ウ 18

エ 21

問20 RAIDにおいて，信頼性向上ではなく，性能向上だけを目的としたものはどれか。

ア RAID0

イ RAID1

ウ RAID3

エ RAID5

問21 オンラインシステムの障害対策に関する記述のうち、適切なものはどれか。

- ア ジャーナルファイルやマスタファイルのバックアップファイルは、すぐに復旧処理ができるようにオリジナルファイルと同一の場所に保管する。
- イ トランザクションの処理が正常に終了できなかったときは、トランザクション開始直前の状態に戻すために、ロールフォワード処理を実行する。
- ウ マスタファイルと一定時間ごとに作成したマスタファイル更新用のトランザクションファイルを用いて、システム障害発生直前の最新データを復元する。
- エ マスタファイルは、オンライン処理の終了時にバックアップファイルを取るだけでなく、システムの特性に応じた時期にバックアップファイルを取る。

問22 システムを本番運用に移行する前に、移行テストを実施することになった。運用部門の担当者の役割として、適切なものはどれか。

- ア 移行時の特殊な利用形態においても、本番業務に支障がないことを確認する。
- イ 移行の作業手順を検討し、移行用マシンのシステム環境を準備する。
- ウ 提供するハードウェアやソフトウェアが正しく動作することを確認する。
- エ 本番用のデータやプログラムが、計画どおりに正しく移行されるかどうかを確認する。

問23 ネットワークシステムの管理・運用に関する記述のうち、適切なものはどれか。

- ア 運用管理者は、各種ネットワーク機器の使用に対する課金管理機能を準備しておく必要がある。
- イ 障害の発生・回復に関する情報収集は膨大なデータ量になるので、システムが安定稼働した時点でこれらの障害管理機能の利用頻度を低くする。
- ウ 転送誤り数、稼働状況などを監視する性能管理機能は、導入当初は必要であるが、システムが安定稼働すると不要になる。
- エ パケット転送に必要な経路管理テーブル類は運用上重要であり、日常の監視が必要である。

問24 データベース管理者は“データベースの総合的な管理”を行う。一方、データ管理者は“組織全体のデータ管理”と“情報資源全体の方針、戦略、計画の作成”を行う。データベース管理者の仕事はどれか。

- ア 各種データベースの利用又は操作の対象を記述したデータ（メタデータ）の作成と管理
- イ 情報システムの対象業務に関するデータの安全性（セキュリティ）確保のためのポリシーの策定
- ウ 情報システムの対象業務に関するデータの標準化
- エ 情報システムのデータベースへのアクセス制御機構とアクセス手順の確立

問25 顧客サービスの運用業務において、システム監査を受ける際の運用責任者の対応として、適切なものはどれか。

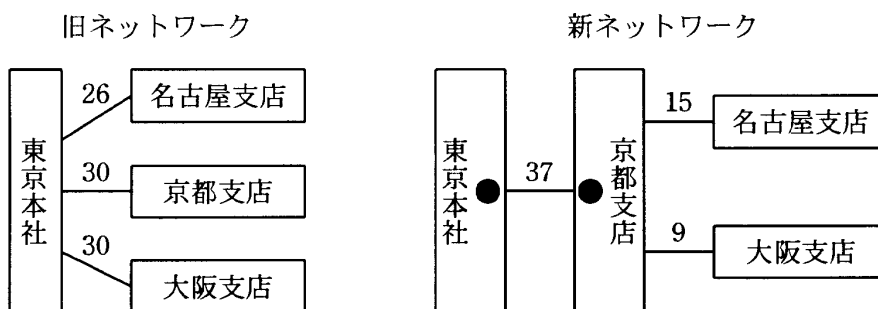
ア システム監査人から建物の障害対策について問われたとき、システム監査の対象は情報システムの運用にかかわるソフトウェア、ハードウェア及びネットワークの管理であり、監査の対象外である旨を説明した。

イ システム監査人からデータ管理ルールを変更すべきという勧告があったが、自分の考えと違うので変更しなかった。

ウ トラブルに関しては、発生から復旧まで電子メールでやりとりした結果を保管し、管理表にはトラブルの概要、発生日及び復旧日を記入するルールとしている。監査人から内容を聞かれたので、電子メールの内容をルールに従って答えた。

エ 利用者情報の閲覧は申請書に基づいて管理するルールになっている。申請書中の担当者の記入漏れを指摘されたとき、運用責任者は担当者を特定できるので記入の省略を許している旨を答えた。

問26 東京本社と各支店間を直接接続している通信ネットワークに、回線多重化装置（図の●印）を導入し、通信ネットワークのコストダウンを図った。このときの月額経済効果は何万円か。ここで、新旧ネットワークの各支店間の月額回線費用（万円）は図に示すとおりである。また、回線多重化装置は1台300万円の装置を月額料率2%のリース契約で2台導入することにし、モデムなどの通信装置の金額は無視する。



ア 10

イ 13

ウ 15

エ 19

問27 重要性や需要変動，在庫コストの観点から定量発注法，定期発注法，2ピン発注法のいずれの方法にするかを決定したい。発注方式を決定するために用いる手法として，適切なものはどれか。

- | | |
|--------------------|---------|
| ア ABC 分析（Grade 分析） | イ 管理図 |
| ウ クリティカルパスメソッド | エ 線形計画法 |

問28 ミッションクリティカルシステムの意味として，適切なものはどれか。

- ア OS などのように，業務システムを稼働させる上で必要不可欠なシステム
- イ システム運用条件が，性能の限界に近い状態の下で稼働するシステム
- ウ 障害が起きると，基幹業務に重大な影響を及ぼすようなシステム
- エ 先行して試験導入され，成功すると本格的に導入されるシステム

問29 セキュリティを強化するための案を四つ作成し、次の式で評価することにした。

$$\text{総合評価点} = \text{効果の評価の合計} - \text{リスクの評価の合計}$$

最も総合評価点の高い強化案はどれか。ここで、効果の評価、リスクの評価はそれぞれ基準表に従って重み付けをするものとする。

効果評価用の基準表

効果	評価点	重み
セキュリティ強化	低い(1点)～高い(5点)	4
システム運用品質向上	低い(1点)～高い(5点)	2
作業プロセスコスト削減	低い(1点)～高い(5点)	3

リスク評価用の基準表

リスク	配点	重み
システム作成費用	小規模(1点)～大規模(5点)	8
技術リスク	業界標準(1点)～新技術(5点)	3

強化案の採点表

項目 \ 案				
	案1	案2	案3	案4
セキュリティ強化	3	4	5	2
システム運用品質向上	2	4	2	5
作業プロセスコスト削減	5	4	2	4
システム作成費用	2	4	1	5
技術リスク	4	1	5	1

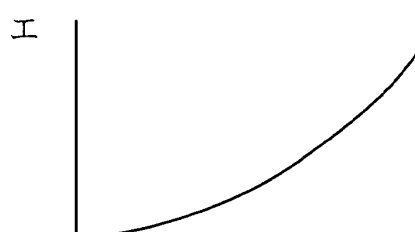
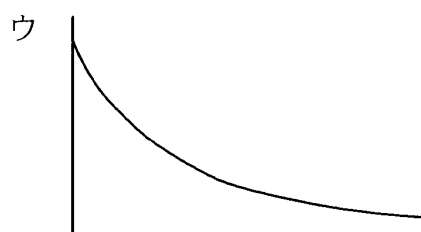
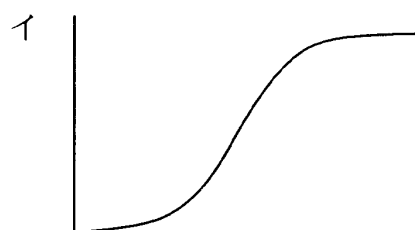
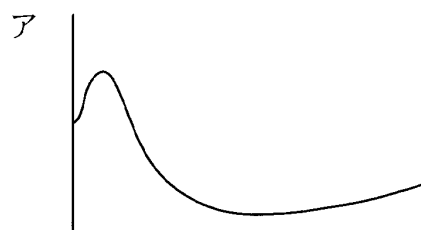
ア 案1

イ 案2

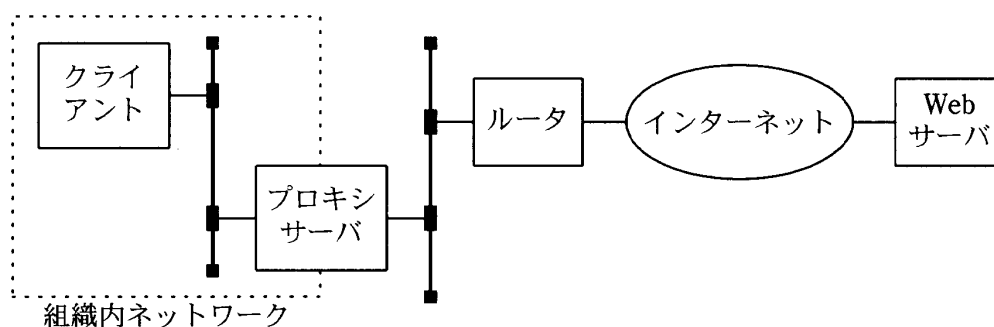
ウ 案3

エ 案4

問30 自社でアプリケーションソフトウェアを開発した。使用中の修正保守，予防保守，適合保守を考慮に入れたソフトウェア保守費用の推移を表したグラフとして，適切なものはどれか。ここで，グラフの横軸は使用開始から使用停止までの経過時間，縦軸は単位期間当たりの保守費用とする。



問31 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32 IP ネットワークのプロトコルのうち，OSI 基本参照モデルのトランスポート層に属するものはどれか。

- ア HTTP イ ICMP ウ SMTP エ UDP

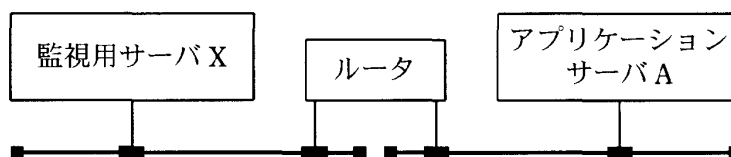
問33 内容の機密性を高めるために用いられる電子メールのプロトコルはどれか。

- ア IMAP4 イ POP3 ウ SMTP エ S/MIME

問34 パケット交換とフレームリレーの比較に関する記述のうち、適切なものはどれか。

- ア ともに蓄積交換によるデータ伝送方式であるが、網内のトラフィックが急増した場合、フレームリレーの方がフレームの廃棄が生じにくい。
- イ パケット交換では、相手先を固定にすることも接続時に選択することもできるが、フレームリレーでは、相手先固定に限定される。
- ウ パケット交換では、送信側から受信側へのパケットの伝送順序が保証されるが、フレームリレーでは、高速化を実現するためにデータの順序は保証されない。
- エ フレームリレーは、パケット交換に比べて誤り制御処理を簡略化することで、網内遅延を少なくし高速化を図っている。

問35 図で示したネットワーク構成において、アプリケーションサーバ A 上の DBMS のデーモンが異常終了したという事象とその理由を、監視用サーバ X で検知するのに有効な手段はどれか。



- ア アプリケーションサーバ A から監視用サーバ X への ICMP あて先到達不能 (Destination Unreachable) メッセージ
- イ アプリケーションサーバ A から監視用サーバ X への SNMP Trap PDU
- ウ 監視用サーバ X からアプリケーションサーバ A への finger
- エ 監視用サーバ X からアプリケーションサーバ A への ping

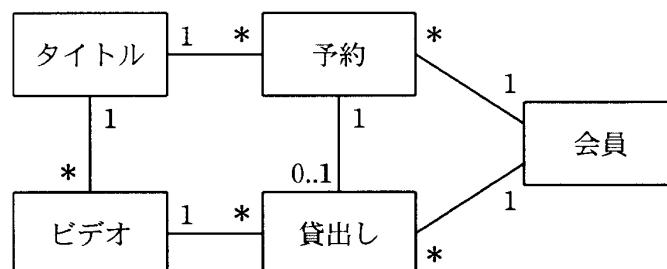
問36 受注入力システムによって作成される次の表の説明として、正しいものはどれか。

受注番号は受注ごとに新たに発行される番号であり、項番は1回の受注で複数の商品の注文があった場合に、商品別に連番で発行される番号である。ここで、受注日、受注番号、項番は入力システムによって自動的に設定される。得意先コード、商品コード、数量は操作員によって入力される項目であり、単価は商品コードに対応したものが台帳から参照される。

受注日	受注番号	得意先コード	項番	商品コード	数量	単価
2005-03-05	995867	0256	1	20121	20	20,000
2005-03-05	995867	0256	2	24005	10	15,000
2005-03-05	995867	0256	3	28007	5	5,000

- ア 正規化は行われていない。
- イ 第1正規化だけ行われている。
- ウ 第2正規化まで行われている。
- エ 第3正規化まで行われている。

問37 ビデオ貸出業務の概念データモデルにおける多重度の解釈として、適切なものはどれか。ここで、長方形はエンティティセットを表し、その中にその名称を記す。長方形間の線は関連を表す。関連の多重度を関連先の近傍に付す。多重度の下限値及び上限値を特に指定する場合は、“下限..上限”の形式とし、“*”は0以上を示す。



- ア タイトルのないビデオも存在する。
- イ ビデオが存在していなくても予約ができる。
- ウ 予約したビデオは必ず貸し出される。
- エ 予約をしなくてもビデオは借りられる。

問38 二つの表“商品”、“在庫”に対する次の SQL 文と、同じ結果が得られる SQL 文はどれか。

```
SELECT 商品番号 FROM 商品
WHERE 商品番号 NOT IN (SELECT 商品番号 FROM 在庫)
```

商品			在庫		
商品番号	商品名	単価	在庫番号	商品番号	在庫数

- ア SELECT 商品番号 FROM 在庫
WHERE EXISTS (SELECT 商品番号 FROM 商品)
- イ SELECT 商品番号 FROM 在庫
WHERE NOT EXISTS (SELECT 商品番号 FROM 商品)
- ウ SELECT 商品番号 FROM 商品
WHERE EXISTS (SELECT 商品番号 FROM 在庫
WHERE 商品.商品番号 = 在庫.商品番号)
- エ SELECT 商品番号 FROM 商品
WHERE NOT EXISTS (SELECT 商品番号 FROM 在庫
WHERE 商品.商品番号 = 在庫.商品番号)

問39 トランザクション A と B が、共通の資源であるテーブル a と b を表に示すように更新するとき、デッドロックとなるのはどの時点か。ここで、表中の番号は処理の実行順序を示す。また、ロックはテーブルの更新直前にテーブル単位で行い、アンロックはトランザクション終了時に行うものとする。

	トランザクション A	トランザクション B
時間 ↓	① トランザクション開始	② トランザクション開始
	③ テーブル a 更新	④ テーブル b 更新
	⑤ テーブル b 更新	⑥ テーブル a 更新
	⑦ トランザクション終了	⑧ トランザクション終了

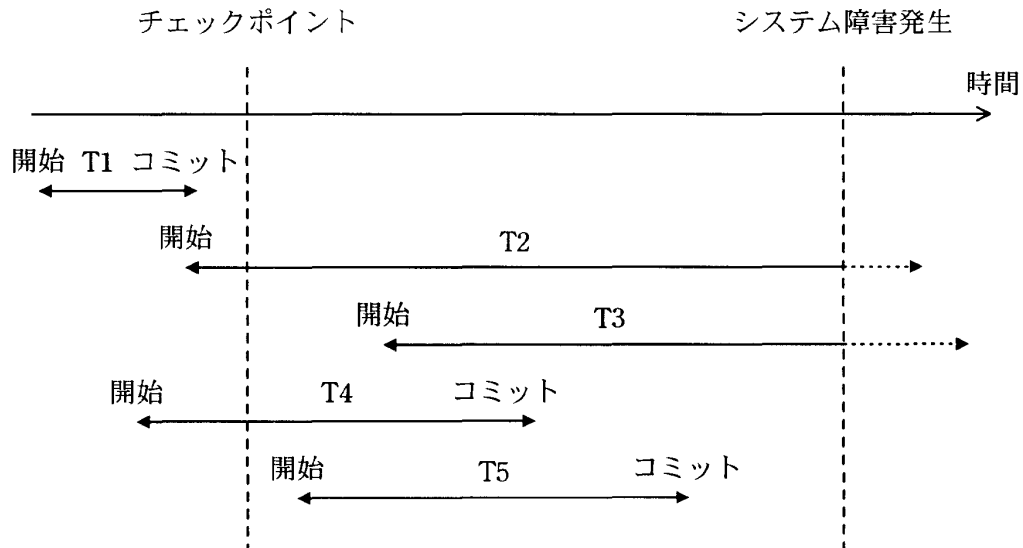
ア ③

イ ④

ウ ⑤

エ ⑥

問40 チェックポイントを取得する DBMS において，図のような時間経過でシステム障害が発生した。前進復帰（ロールフォワード）によって障害回復できるすべてのトランザクションはどれか。



- ア T1 イ T2 と T3 ウ T4 と T5 エ T5

問41 共通かぎ暗号方式のかぎとして 32 ビットのかぎを使用した場合，かぎの候補は何通りか。

- ア 32^2 イ $32!$ ウ 2^{32} エ ${}_{32}C_2$

問42 X さんは，Y さんにインターネットを使って電子メールを送ろうとしている。電子メールの内容は秘密にする必要があるので，公開かぎ暗号方式を使って暗号化して送信したい。電子メールの内容を暗号化するのに使用するかぎはどれか。

- ア X さんの公開かぎ イ X さんの秘密かぎ
ウ Y さんの公開かぎ エ Y さんの秘密かぎ

問43 ハッシュ関数を利用したメッセージ認証に関する記述のうち、適切なものはどれか。

- ア 受信者は、送信者の公開かぎとハッシュ関数を用いてハッシュ値からメッセージを復号する。
- イ 受信者は、ハッシュ関数を用いてメッセージからハッシュ値を生成し、送信者の公開かぎで復号したハッシュ値と比較する。
- ウ 送信者は、自分の公開かぎとハッシュ関数を用いてメッセージからハッシュ値を生成し、メッセージとともに送信する。
- エ 送信者は、ハッシュ関数を用いて送信者の秘密かぎのハッシュ値を生成し、メッセージとともに送信する。

問44 スパイウェアによって引き起こされた情報の漏えいに該当するものはどれか。

- ア 暗号化せずに電子メールを送信したところ、ネットワーク上で内容が読み取られてしまった。
- イ インターネットに接続したところ、パソコン内の利用者情報が知らないうちに送信されてしまった。
- ウ パスワードを忘れてしまったという電話に対して、システム管理者が教えたのでパスワードが他人に知られてしまった。
- エ パソコンをそのまま廃棄したところ、磁気媒体上に残存していたデータが読み取られてしまった。

問45 情報システムにおけるデータのオーナーに相当する部門として、適切なものはどれか。

- ア システム及びデータの維持管理を行っているシステム運用部門
- イ システム部門に開発，運用及び保守を委託している業務の主管部門
- ウ データのインテグリティを保証し，必要に応じてデータ内容の訂正を行う保守部門
- エ データを取り扱う画面や帳票のレイアウトを決定する利用部門

問46 コンピュータセキュリティ対策に関する記述のうち、適切なものはどれか。

- ア 一時記憶領域に残っている機密データの漏えいに対しては，ジョブ終了時に一時記憶領域のデータを確実に消去する。
- イ 金利計算処理などで，端数を特定口座に振り込む，いわゆるサラミ技術に対しては，データにチェックディジットを付加する。
- ウ 端末から入力された数値データの改ざんに対しては，仮想記憶領域のページ又はセグメント単位に割り付けられた記憶保護キーによって，保護のレベルを変える。
- エ ユーティリティプログラムを使用したデータ改ざんに対しては，そのユーティリティプログラムのバックアップをとっておき，元のプログラムと比較する。

問47 テンペスト技術の説明とその対策として、適切なものはどれか。

- ア ディスプレイなどの機器から放射される電磁波を傍受し、内容を観察する技術であり、電磁波遮断が施された部屋に機器を設置することによって対抗する。
- イ データ通信の途中でパケットを横取りし、内容を改ざんする技術であり、デジタル署名による改ざん検知の仕組みを実装することによって対抗する。
- ウ マクロ型ウイルスに対して使われる技術であり、ウイルス対策ソフトを導入し、最新の定義ファイルを適用することによって対抗する。
- エ 無線 LAN の信号から通信内容を傍受し、解析する技術であり、通信パケットを暗号化することによって対抗する。

問48 ファイアウォールの方式に関する記述のうち、適切なものはどれか。

- ア アプリケーションゲートウェイ方式では、アプリケーションの Protokol ごとにゲートウェイ機能の設定が必要である。
- イ サーキットゲートウェイ方式では、コマンドの通過可否を制御する。
- ウ トランスポートゲートウェイ方式では、アプリケーションの Protokol に依存するゲートウェイ機能を提供する。
- エ パケットフィルタリング方式では、電子メールの中に含まれる単語によるフィルタリングが可能である。

問49 通信の暗号化に関する記述のうち、適切なものはどれか。

- ア IPsec のトランスポートモードでは、ゲートウェイ間の通信経路上だけではなく、発信側システムと受信側システムとの間の全経路上でメッセージが暗号化される。
- イ LDAP クライアントが LDAP サーバに接続するとき、その通信内容は暗号化することができない。
- ウ S/MIME で暗号化した電子メールは、受信側のメールサーバ内に格納されている間は、メール管理者が平文として見ることができる。
- エ SSL を使用して接続したとき、ブラウザのディスクキャッシュ内に格納した HTML 文書は、暗号化したままで保存される。

問50 電子的な方法を用いしないで、緊急事態を装って組織内部の人間からパスワードや機密情報のありかを不正に聞き出して入手する行為は、どれに分類されるか。

- ア ソーシャルエンジニアリング イ トロイの木馬
- ウ パスワードクラック エ 踏み台攻撃

問51 情報システムのリスク分析に関する記述のうち、適切なものはどれか。

- ア リスクには、投機的リスクと純粹リスクとがある。情報セキュリティのためのリスク分析で対象とするのは、投機的リスクである。
- イ リスクの予想損失額は、損害予防のために投入されるコスト、復旧に要するコスト、及びほかの手段で業務を継続するための代替コストの合計で表される。
- ウ リスク分析では、現実が発生すれば損失をもたらすリスクが、情報システムのどこに、どのように潜在しているかを識別し、その影響の大きさを測定する。
- エ リスクを金額で測定するリスク評価額は、損害が現実のものになった場合の 1 回当たりの平均予想損失額で表される。

問52 財団法人日本情報処理開発協会のプライバシーマーク制度について説明したものはどれか。

- ア OECD のプライバシーガイドラインに準拠している公的機関及び民間事業者を認定する制度
- イ 個人情報を買取る事業者が一定の基準を満たしていることを認定する制度
- ウ 個人情報を保有している事業者に個人情報保護措置の概要を登録させる制度
- エ 事業者が個人情報の取扱いを適切に行うための体制などを整備していることを認定する制度

問53 米国で運用された TCSEC や欧州政府調達用の ITSEC を統合して、標準化が進められた CC (Common Criteria) の内容はどれか。

- ア 情報技術に関するセキュリティの評価基準
- イ 情報セキュリティ基礎技術の標準
- ウ セキュリティ管理のプロトコルの標準
- エ 通信サービスに関するセキュリティ機能の標準

問54 ISMS 適合性評価制度における詳細管理策の基となった国際規格はどれか。

- ア ISO 9001 イ ISO 14001 ウ ISO/IEC 15408 エ ISO/IEC 17799

問55 SAML (Security Assertion Markup Language) の説明はどれか。

- ア Web サービスに関する情報を広く公開し、それらが提供する機能などを検索可能にするための仕組みを定めたもの
- イ 権限のない利用者による傍受、読取り、改ざんから電子メールを保護して送信するためのプロトコルを定めたもの
- ウ デジタル署名に使われるかぎ情報を効率よく管理するための Web サービスプロトコルを定めたもの
- エ 認証情報に加え、属性情報とアクセス制御情報を異なるドメインに伝達するための Web サービスプロトコルを定めたもの

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

9. 答案用紙の記入に当たっては、次の指示に従ってください。

- (1) HB の黒鉛筆又はシャープペンシルを使用してください。訂正の場合は、あとが残らないように消しゴムできれいに消し、消しくずを残さないでください。
- (2) 答案用紙は光学式読取り装置で処理しますので、答案用紙のマークの記入方法のとおりマークしてください。
- (3) 受験番号欄に、受験番号を記入及びマークしてください。正しくマークされていない場合、答案用紙のマークの記入方法のとおりマークされていない場合は、採点されません。
- (4) 生年月日欄に、受験票に印字されているとおりの生年月日を記入及びマークしてください。正しくマークされていない場合は、採点されないことがあります。
- (5) 解答は、次の例題にならって、解答欄に一つだけマークしてください。

〔例題〕 春の情報処理技術者試験が実施される月はどれか。

ア 2 イ 3 ウ 4 エ 5

正しい答えは“ウ 4”ですから、次のようにマークしてください。

例題	☐ ア	☐ イ	☒ ウ	☐ エ
----	-------------------------	-------------------------	------------------------------------	-------------------------

10. 試験終了後、この問題冊子は持ち帰ることができます。
11. 答案用紙は、白紙であっても提出してください。
12. 試験時間中にトイレへ行きたくなったり、気分が悪くなったりした場合は、手を挙げて監督員に合図してください。
13. 午後の試験開始は 12:10 ですので、12:00 までに着席してください。

試験問題に記載されている会社名又は製品名は、それぞれ各社の商標又は登録商標です。

なお、試験問題では、® 及び ™ を明記していません。