

問 5 フラグメンテーションに関する記述のうち，適切なものはどれか。

- ア 可変長ブロックのメモリプール管理方式では，様々な大きさのメモリ領域の獲得や返却を行ってもフラグメンテーションは発生しない。
- イ 固定長ブロックのメモリプール管理方式では，可変長ブロックのメモリプール管理方式よりもメモリ領域の獲得と返却を速く行えるが，フラグメンテーションが発生しやすい。
- ウ フラグメンテーションの発生によって，合計としては十分な空きメモリ領域があるにもかかわらず，必要とするメモリ領域を獲得できなくなることがある。
- エ メモリ領域の獲得と返却の頻度が高いシステムでは，フラグメンテーション発生を防止するため，メモリ領域が返却されるたびにガーベジコレクションを行う必要がある。

問 6 M/M/1 の待ち行列モデルにおける，平均待ち時間（ W ）と窓口利用率（ ρ ）の関係で， ρ が 0.25 から 0.75 になったとき， W は何倍になるか。

- ア $\frac{1}{3}$ イ 3 ウ 4.5 エ 9

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 通信事業者が提供する網のうち，LAN で使用するインタフェースをそのままユーザ・網インタフェースとし，ユーザごとに閉域性を確保したものはどれか。

ア ADSL

イ FTTH

ウ 広域イーサネット

エ パケット交換網

問 13 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 14 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 15 コンピュータグラフィックスの要素技術に関する記述のうち，適切なものはどれか。

- ア アンチエイリアシングは周辺の画素との平均化演算などを施し，ギザギザを目立たなくする。
- イ メタボールは物体表面の相互反射を放射エネルギー方程式から直接計算する。
- ウ ラジオシティは光源から物体表面での反射屈折を繰り返し，最終的に視点に入る光源をすべて追跡して計算する。
- エ レイトレーシングは物体を球やだ円体の集合で擬似的にモデル化する。

問 16 フールプルーフに該当するものはどれか。

- ア 更新の対象となるものをコピーして保存する。
- イ 入力したデータの取消し操作を行うことができるようにする。

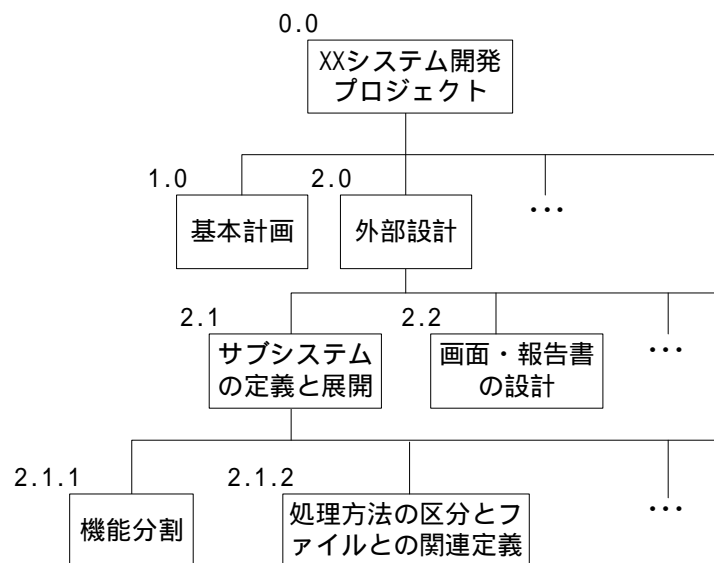
- ウ メニュー画面上の不適切な項目は，選択できないようにする。
- エ 利用者の操作内容をログとして保存する。

問 17 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。

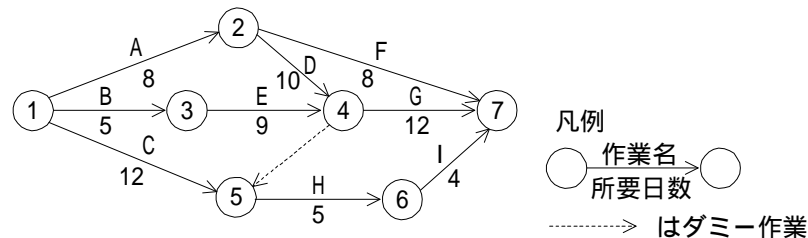
- ア 原因結果グラフ
- イ 限界値分析
- ウ 同値分割
- エ 分岐網羅

問 18 図のように，プロジェクトを大枠から詳細なレベルまでの具体的な作業に分解したものを何というか。



- ア DFD
- イ DOA
- ウ PERT
- エ WBS

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 ANSI/SPARC3層スキーマに関する記述として, 適切でないものはどれか。

- ア ANSI/SPARC3層スキーマの意義は, 物理的データ独立性及び論理的データ独立性を確保することである。
- イ 外部スキーマは, 実世界が変化しても応用プログラムができるだけ影響を受けないようにするための考え方である。
- ウ 関係データベースのビューやネットワークデータベースのサブスキーマは, 概念スキーマに相当する。
- エ 内部スキーマは, 直接編成ファイルや VSAM ファイルなどの物理ファイルを用いて, 概念スキーマをコンピュータ上に実装するための記述である。

問22 関係データベースにおける定義域に関する記述のうち, 適切なものはどれか。

- ア 定義域が異なる属性同士の比較は, 本質的には意味がない。
- イ 定義域は, 単一の基本データ型又はユーザ定義型でなければならない。
- ウ 定義域は, ユーザ定義のスキーマである。
- エ 一つの属性は, 複数の定義域上に定義できなければならない。

問 23 次の関係 “注文” の属性に ~ の関数従属性があるとき，主キー属性の組として正しいものはどれか。ここで，(A, B) という記述は，属性 A と B の組を表す。また，A C という記述は，C が A に関数従属していることを表す。

関係 “注文”

(注文番号，注文日，顧客番号，顧客名，商品番号，商品名，数量，金額)

関数従属性

注文番号	注文日	注文番号	顧客番号
注文番号	顧客名	顧客番号	顧客名
(注文番号，商品番号)	数量	(注文番号，商品番号)	金額
商品番号	商品名		

- ア (注文番号)
- イ (注文番号，顧客番号)
- ウ (注文番号，顧客番号，商品番号)
- エ (注文番号，商品番号)

問 24 関数従属に関する記述のうち，適切なものはどれか。ここで，A, B, C はある関係の属性の集合とする。

- ア B が A に関数従属し，C が A に関数従属すれば，C は B に関数従属する。
- イ B が A の部分集合であり，C が A に関数従属すれば，C は B に関数従属する。
- ウ B が A の部分集合であれば，A は B に関数従属する。
- エ B と C の和集合が A に関数従属すれば，B と C はそれぞれが A に関数従属する。

問 25 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 26 次の表を,第3正規形まで正規化を行った場合,幾つの表に分割されるか。ここで,顧客の1回の注文に対して1枚の受注伝票が作られ,顧客は1回の注文で一つ以上の商品を注文できるものとする。

受注番号	顧客コード	顧客名	受注日	商品コード	商品名	単価	受注数	受注金額
1055	A7053	鈴木電気	2004-07-01	T035	テレビ A	85,000	10	850,000
1055	A7053	鈴木電気	2004-07-01	K083	ラジカセ A	23,000	5	115,000
1055	A7053	鈴木電気	2004-07-01	S172	ステレオ B	78,000	3	234,000
2030	B7060	中村商会	2004-07-03	T050	テレビ B	90,000	3	270,000
2030	B7060	中村商会	2004-07-03	S172	ステレオ B	78,000	10	780,000
3025	C9025	佐藤電気	2004-07-03	T035	テレビ A	85,000	3	255,000
3025	C9025	佐藤電気	2004-07-03	K085	ラジカセ B	25,000	2	50,000
3025	C9025	佐藤電気	2004-07-03	S171	ステレオ A	50,000	8	400,000
3090	B7060	中村商会	2004-07-04	T050	テレビ B	90,000	1	90,000
3090	B7060	中村商会	2004-07-04	T035	テレビ A	85,000	2	170,000

- ア 2
- イ 3
- ウ 4
- エ 5

問27 SQL文のSELECT句に関する記述として、適切なものはどれか。

- ア FROM句で指定した表の列以外のものを指定できない。
- イ 重複を排除した検索結果を作ることはいできない。
- ウ 同一の列を重複して指定できる。
- エ 表のすべての列を得るには、すべての列をコンマで区切って指定しなければならない。

問28 “履修”表と“担当”表を自然結合した結果表はどれか。

履修

学生	科目
山田太郎	情報処理
山田太郎	代数
加藤花子	情報処理

担当

科目	教官
情報処理	鈴木一郎
代数	斎藤正樹

- ア
- | 学生 | 科目 | 教官 |
|------|------|------|
| 山田太郎 | 情報処理 | 鈴木一郎 |
| 山田太郎 | 代数 | 斎藤正樹 |
| 加藤花子 | 情報処理 | 鈴木一郎 |
- イ
- | 履修.学生 | 履修.科目 | 担当.科目 | 担当.教官 |
|-------|-------|-------|-------|
| 山田太郎 | 情報処理 | 情報処理 | 鈴木一郎 |
| 山田太郎 | 代数 | 代数 | 斎藤正樹 |
| 加藤花子 | 情報処理 | 情報処理 | 鈴木一郎 |
- ウ
- | 履修.学生 | 履修.科目 | 担当.科目 | 担当.教官 |
|-------|-------|-------|-------|
| 山田太郎 | 情報処理 | 代数 | 斎藤正樹 |
| 山田太郎 | 代数 | 情報処理 | 鈴木一郎 |
| 加藤花子 | 情報処理 | 代数 | 斎藤正樹 |
- エ
- | 履修.学生 | 履修.科目 | 担当.科目 | 担当.教官 |
|-------|-------|-------|-------|
| 山田太郎 | 情報処理 | 情報処理 | 鈴木一郎 |
| 山田太郎 | 情報処理 | 代数 | 斎藤正樹 |
| 山田太郎 | 代数 | 情報処理 | 鈴木一郎 |
| 山田太郎 | 代数 | 代数 | 斎藤正樹 |
| 加藤花子 | 情報処理 | 情報処理 | 鈴木一郎 |
| 加藤花子 | 情報処理 | 代数 | 斎藤正樹 |

問 29 関係 R と S において $R \div S$ の関係演算結果として適切なものはどれか。ここで \div は除算を表す。

店	商品
A	a
A	b
B	a
B	b
B	c
C	c
D	c
D	d
E	d
E	e

商品
a
b
c

店
A
A
B
B
B
C
D

店
A
B
C
D

店
B

店
E

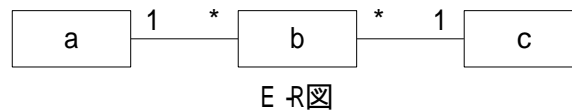
問 30 関係データモデルにおいて属性 A, B を考える。属性 A のドメイン（定義域）は m 個の要素からなる集合であり，属性 B のドメインは n 個の要素からなる集合であるとする。このとき，関係 R を $R(A, B)$ とすると，R には最大何個のタプルがあるか。

- ア $2^m 2^n$ イ $(m+n)^2$ ウ $m+n$ エ mn

問 31 部品在庫管理台帳における, 部品, 仕入先, 在庫の三つのエンティティの関係を E-R 図として記述した。エンティティ a~c の組合せとして, 適切なものはどれか。ここで, 1 * は 1 対多のカーディナリティを表す。

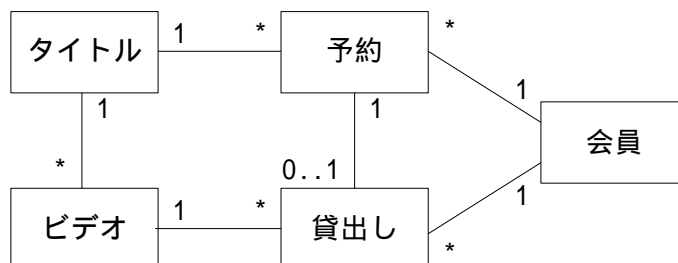
部品在庫管理台帳

部品コード	部品名	仕入先コード	仕入先名	仕入日付	仕入価格	在庫数
001	R 部品	Z010	P 商会	9 月 1 日	1,500	1,000
001	R 部品	Z010	P 商会	10 月 15 日	1,400	1,500
002	S 部品	Z010	P 商会	9 月 20 日	800	500
003	T 部品	Z015	Q 商店	10 月 8 日	1,600	1,450



	A	b	c
ア	在庫	仕入先	部品
イ	在庫	部品	仕入先
ウ	仕入先	部品	在庫
エ	部品	在庫	仕入先

問 32 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33 次のSQL文は, COBOL プログラムでテーブルAのレコードを読み込むためにカーソル宣言をしている。aに入れるべき適切な語句はどれか。

a

```
SELECT * FROM A
      ORDER BY 1, 2
END-EXEC
```

- ア EXEC SQL DECLARE C1 CURSOR FOR
- イ EXEC SQL DECLARE CURSOR FOR C1
- ウ EXEC SQL OPEN CURSOR C1 FOR
- エ EXEC SQL OPEN CURSOR DECLARE C1 FOR

問34 “会員”表に対し次のSQL文を実行した結果として, 正しいものはどれか。

```
SELECT X.会員名
      FROM 会員 X, 会員 Y
      WHERE X.リーダ会員番号 = Y.会員番号
            AND X.生年月日 < Y.生年月日
```

会員

会員番号	会員名	生年月日	リーダ会員番号
001	田中	1960-03-25	002
002	鈴木	1970-02-15	002
003	佐藤	1975-05-27	002
004	福田	1960-10-25	004
005	渡辺	1945-09-01	004

- ア

会員名
(該当者なし)
- イ

会員名
佐藤
- ウ

会員名
鈴木
福田
- エ

会員名
田中
渡辺

問35 “部品”表に対し次のSELECT文を実行したときの結果として, 正しいものはどれか。

```
SELECT 部品区分, COUNT(*) AS 部品数, MAX(単価) AS 単価
FROM 部品 GROUP BY 部品区分 HAVING SUM(在庫量) > 200
```

部品

部品番号	部品区分	単価	在庫量
001	P1	1,500	90
002	P2	900	30
003	P2	950	90
004	P3	2,000	50
005	P1	2,000	100
006	P3	2,500	60
007	P1	1,500	50
008	P2	900	80
009	P3	1,000	40
010	P4	900	80
011	P3	1,500	70
012	P4	950	100

ア

部品区分	部品数	単価
P1	3	2,000
P2	3	1,000

イ

部品区分	部品数	単価
P1	3	2,000
P3	4	2,500

ウ

部品区分	部品数	単価
P2	3	1,000
P4	2	950

エ

部品区分	部品数	単価
P1	3	2,000
P2	3	1,000
P3	4	2,500

問 36 “製品”表と“在庫”表に対し, 次の SQL 文を実行した結果として得られる表の行数は幾つか。

```
SELECT 製品番号 FROM 製品
WHERE NOT EXISTS( SELECT 製品番号 FROM 在庫
WHERE 在庫数 > 30 AND 製品.製品番号 = 在庫.製品番号)
```

製品

製品番号	製品名	単価
AB1805	CD-ROM ドライブ	15,000
CC5001	デジタルカメラ	65,000
MZ1000	プリンタ A	54,000
XZ3000	プリンタ B	78,000
ZZ9900	イメージスキャナ	98,000

在庫

倉庫コード	製品番号	在庫数
WH100	AB1805	20
WH100	CC5001	200
WH100	ZZ9900	130
WH101	AB1805	150
WH101	XZ3000	30
WH102	XZ3000	20
WH102	ZZ9900	10
WH103	CC5001	40

- ア 1 イ 2 ウ 3 エ 4

問 37 二つの表“納品”, “顧客”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 顧客番号, 顧客名 FROM 顧客
WHERE 顧客番号 IN
( SELECT 顧客番号 FROM 納品
WHERE 商品番号 = 'G1' )
```

納品

商品番号	顧客番号	納品数量
------	------	------

顧客

顧客番号	顧客名
------	-----

- ア SELECT 顧客番号, 顧客名 FROM 顧客
 WHERE 'G' IN (SELECT 商品番号 FROM 納品)
- イ SELECT 顧客番号, 顧客名 FROM 顧客
 WHERE 商品番号 IN
 (SELECT 商品番号 FROM 納品
 WHERE 商品番号 = 'G1')
- ウ SELECT 顧客番号, 顧客名 FROM 納品, 顧客
 WHERE 商品番号 = 'G1'
- エ SELECT 顧客番号, 顧客名 FROM 納品, 顧客
 WHERE 納品.顧客番号 = 顧客.顧客番号 AND 商品番号 = 'G1'

問 38 A 社では，社員教育の一環として全社員を対象に英会話研修を行っていたが，本年度（2005 年度）からは，4 月時点で入社 3 年を経過しているにもかかわらず初級システムアドミニストレータ（初級シスアド）試験に合格していない技術職種の社員に対して，英会話の代わりに初級シスアド研修を受講させることにした。本年度の英会話研修を受講させる社員の一覧を出力するための SQL 文はどれか。

なお，A 社では，社員はすべて 4 月 1 日入社であり，事業年度の始まりは 4 月 1 日である。また，ここで使用するデータベースには，2005 年 4 月 1 日時点でのデータが格納されているものとする。

ア SELECT 社員 FROM 社員テーブル

WHERE (入社年度 <= (2005 - 3) AND 職種 = '技術')
AND 初級シスアド合格 = 'No'

イ SELECT 社員 FROM 社員テーブル

WHERE (入社年度 <= (2005 - 3) AND 職種 = '技術')
OR 初級シスアド合格 = 'Yes'

ウ SELECT 社員 FROM 社員テーブル

WHERE NOT (入社年度 <= (2005 - 3) AND 職種 = '技術')
AND 初級シスアド合格 = 'No'

エ SELECT 社員 FROM 社員テーブル

WHERE NOT (入社年度 <= (2005-3) AND 職種 = '技術')
OR 初級シスアド合格 = 'Yes'

問 39 DBMS において，デッドロックを検出するために使われるデータ構造はどれか。

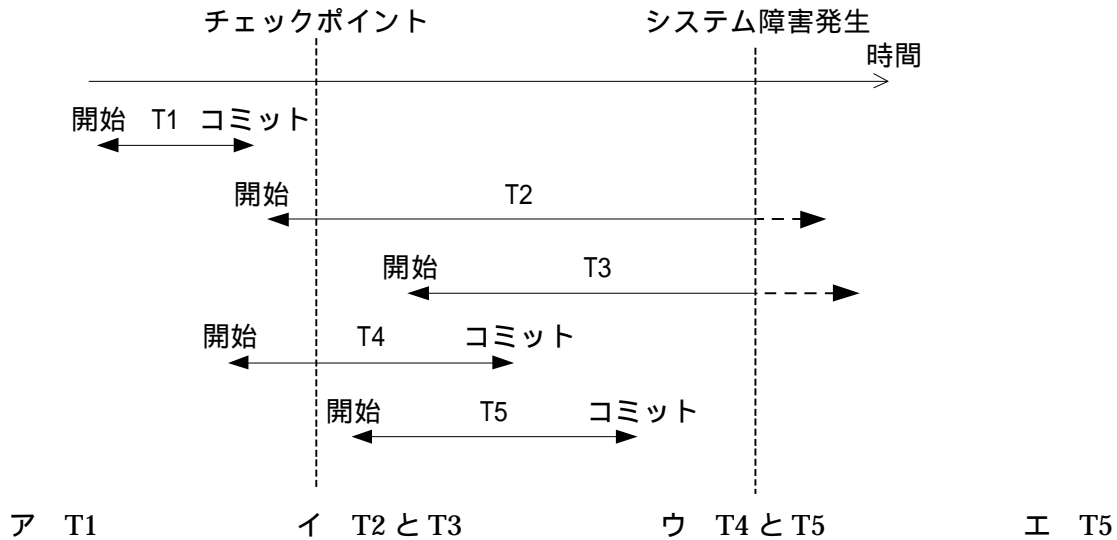
ア 資源割当表

イ 時刻印順管理表

ウ トランザクションの優先順管理表

エ 待ちグラフ

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。



問41 分散データベースのトランザクションは複数のサブトランザクションに分割され, 複数のサイトで実行される。このとき, トランザクションのコミット制御に関する記述のうち, 適切なものはどれか。

- ア 2相コミットでは, すべてのサブトランザクションからコミット了承応答が届いても, 必ずしもすべてのサブトランザクションをコミットするとは限らない。
- イ 2相コミットを用いても, サブトランザクションが実行されるサイトに主サイトの指示が届かず, サブトランザクションをコミットすべきかロールバックすべきか分からない場合がある。
- ウ 2相コミットを用いると, サブトランザクションがロールバックされてもトランザクションがコミットされる場合がある。
- エ 集中型データベースのコミット制御である1相コミットで, 個々のサイトが独自に分散データベースのコミットを行っても, サイト間のデータベースの一貫性は保証できる。

問42 DBMSに実装すべき原子性(atomicity)の説明として, 適切なものはどれか。

- ア 同一データベースに対する同一処理は, 何度実行しても結果は同じである。
- イ トランザクションが完了すると, その後にハードウェア障害が発生しても, 更新されたデータベース内容は保証される。
- ウ トランザクション内の処理は, すべてが実行されるか, 全く実行されないかのいずれかしかない。

エ 一つのトランザクションの処理結果は, ほかのトランザクション処理の影響を受けることはない。

問 43 二つのトランザクション T1, T2 が, データ a, b を平行してアクセスする。T1, T2 の組合せのうち, 直列可能性が保証できるものはどれか。ここで, トランザクションの各操作の意味は次のとおりとする。

LOCK x : データ x をロックする
 READ x : データ x を読み込む
 STORE x : データ x を書き出す
 UNLOCK x : データ x をアンロックする

ア	T1	T2	イ	T1	T2
	READ a	READ a		LOCK a	LOCK a
	LOCK a	LOCK a		READ a	READ a
	LOCK b	LOCK b		a = a + 3	a = a + 3
	a = a + 3	a = a + 3		STORE a	STORE a
	STORE a	STORE a		UNLOCK a	UNLOCK a
	READ b	READ b		LOCK b	LOCK b
	b = b + 5	b = b + 5		READ b	READ b
	STORE b	STORE b		b = b + 5	b = b + 5
	UNLOCK a	UNLOCK a		STORE b	STORE b
	UNLOCK b	UNLOCK b		UNLOCK b	UNLOCK b
ウ	T1	T2	エ	T1	T2
	LOCK a	LOCK a		LOCK a	LOCK a
	READ a	READ a		READ a	READ a
	a = a + 3	LOCK b		a = a + 3	LOCK b
	STORE a	READ b		STORE a	READ b
	UNLOCK a	UNLOCK a		LOCK b	UNLOCK b
	LOCK b	UNLOCK b		READ b	UNLOCK a
	READ b			b = b + 5	
	b = b + 5			STORE b	
	STORE b			UNLOCK b	
	UNLOCK b			UNLOCK a	

問 44 分散データベースシステムにおける問合せでは，サイト間にまたがる結合演算の最適化が重要である。この最適化の方法として，適切なものはどれか。

- ア LRU 法 イ セミジョイン法 ウ ソートマージ法 エ 楽観的方法

問 45 一つの表に大量のデータを格納するとき，並列処理のために異なったディスクにデータを分割格納することがある。このような方式のうちキーレンジ分割方式に関する説明はどれか。

- ア 主キーと外部キーの参照関係を保持し，関数従属性に従って異なった表に分割格納する。
イ データの発生した順に格納するディスクを変え，ディスクごとのデータ量が均等になるように分割格納する。
ウ 分割に使用するキーの値にハッシュ関数を適用し，その値に割り当てられたディスクに分割格納する。
エ 分割に使用するキーの値をあらかじめ決めておき，その値に割り当てられたディスクに分割格納する。

問 46 100 人の送受信者が共通かぎ暗号方式で，それぞれ秘密に通信を行うときに必要な暗号かぎの総数は幾つか。

- ア 200 イ 4,950 ウ 9,900 エ 10,000

問 47 通信文を公開かぎ暗号方式によって暗号化し，正規の受信者だけが内容を見ることができ，更に，送信者の認証も行えるようにしたい。この要件を実現する方式のうち，適切なものはどれか。ここで，送信者を A，受信者を B とし，A の公開かぎ及び秘密かぎをそれぞれ a_1 ， a_2 とし，B の公開かぎ及び秘密かぎをそれぞれ b_1 ， b_2 とする。

- ア A は，通信文，及び a_2 で暗号化した署名をまとめて b_1 で暗号化し，送信する。B は， b_2 でまず全体を復号し，更に，暗号化された署名を a_1 で復号し，通信文と署名が正しいことを検証する。
イ A は，通信文，及び b_1 で暗号化した署名をまとめて b_1 で暗号化し，送信する。B は， b_2 でまず全体を復号し，更に，暗号化された署名を b_2 で復号し，通信文と署名が正しいことを検証する。
ウ A は，通信文と署名をまとめて a_2 で暗号化し，送信する。B は， a_1 で復号し，通信文と署名が正しいことを検証する。

エ A は，通信文と署名をまとめて b1 で暗号化し，送信する。B は，b2 で復号し，通信文と署名が正しいことを検証する。

問 48 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 49 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 50 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プロトコル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プロトコル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 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 個人情報を買収す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 SLCP-JCF98(Software Life Cycle Processes-Japan Common Frame 98)策定の目的はどれか。

- ア 取得者と供給者の二者間取引におけるシステムの使用開始から終了までの使用条件を定めること
- イ 取得者と供給者の二者間取引に共通の物差しを用いて取引を明確化すること
- ウ 取得者と供給者の二者間取引の契約条件をパターン化すること
- エ 取得者と供給者の二者間取引のトラブルを回避するためのガイドラインを定めること

問 54 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 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