平成18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

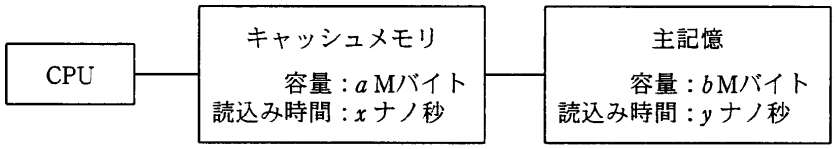
5. 問題は，次の表に従って解答してください。

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。
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　図のアーキテクチャのシステムにおいて，CPU からみた，主記憶とキャッシュメモリを合わせた平均読込み時間を表す式はどれか。ここで，読み込みたいデータがキャッシュメモリに**存在しない確率**を r とし，キャッシュメモリ管理に関するオーバヘッドは無視できるものとする。



ア　$\frac{(1-r)\cdot a}{a+b}\cdot x+\frac{r\cdot b}{a+b}\cdot y$　　イ　$(1-r)\cdot x+r\cdot y$

ウ　$\frac{r\cdot a}{a+b}\cdot x+\frac{(1-r)\cdot b}{a+b}\cdot y$　　エ　$r\cdot x+(1-r)\cdot y$

問2　ベクトルコンピュータの演算性能指標として使われるものはどれか。

ア　Dhrystone　　イ　FLOPS　　ウ　MIPS　　エ　SPECint

問3　二つのタスクが共用する二つの資源を排他的に使用するとき，デッドロックが発生する可能性がある。このデッドロックの発生を防ぐ方法はどれか。

ア　一方のタスクの優先度を高くする。
イ　資源獲得の順序を両方のタスクで同じにする。
ウ　資源獲得の順序を両方のタスクで逆にする。
エ　両方のタスクの優先度を同じにする。

問4　メモリリークに関する記述として，適切なものはどれか。

ア　アプリケーションの同時実行数を増やした場合に，主記憶容量が不足し，処理時間のほとんどがページングに費やされ，極端なスループットの低下を招くことである。

イ　アプリケーションや OS のバグなどが原因で，動作中に確保した主記憶が解放されないことであり，これが発生すると主記憶中の利用できる部分が減少する。

ウ　実行時のプログラム領域の大きさに制限があるときに，必要になったモジュールを主記憶に取り込む手法である。

エ　主記憶の内容と補助記憶の内容とを交換する処理のことである。

問5　関係データベースを用いた 2 層クライアントサーバシステムにおいて，ストアドプロシージャを使わないとき，SQL メッセージを送信するものはどれか。

ア　アプリケーションサーバ

イ　アプリケーションサーバとクライアント

ウ　クライアント

エ　データベースサーバ

問6　クライアントサーバシステムの 3 層アーキテクチャを説明したものはどれか。

ア　アプリケーションに必要な GUI と API をプレゼンテーション層とファンクション層に分離したアーキテクチャであり，データベースサーバを独立させている。

イ　プレゼンテーション層，ファンクション層，データ層に分離したアーキテクチャであり，各層の OS は異なってもよい。

ウ　プレゼンテーション層とデータ層をミドルウェア層によって連係したアーキテクチャであり，各層をネットワークで接続されたコンピュータに分散する。

エ　プレゼンテーション層とファンクション層を結合し，データ層を分離したアーキテクチャであり，データベースサーバを効率的に運用できる。

問7　ページング方式の仮想記憶において，あるプログラムを実行したとき，1 回のページフォールトの平均処理時間は 30 ミリ秒であった。ページフォールト発生時の処理時間が次の条件であったとすると，ページアウトを伴わないページインだけの処理の割合は幾らか。

〔ページフォールト発生時の処理時間〕

(1) ページアウトを伴わない場合，ページインの処理で 20 ミリ秒かかる。

(2) ページアウトを伴う場合，置換えページの選択，ページアウト，ページインの処理で合計 60 ミリ秒かかる。

ア　0.25　　イ　0.33　　ウ　0.67　　エ　0.75

問8　ある金融機関の ATM（現金自動預払機）が 1 台設置されている。平日の昼休み時（12 時から 13 時）には，この ATM を毎日平均 15 人が 1 人当たり平均 3 分の操作時間で利用している。サービス待ちが M/M/1 の待ち行列モデルに従うとすれば，この時間帯の平均待ち時間は何分か。

ア　3　　イ　6　　ウ　9　　エ　12

問9　複数のクライアントから呼び出されるあるサーバのタスク処理時間は，タスクの多重度が 2 以下の場合，常に 4 秒である。このタスクへ 1 秒ずつずれて 4 件の処理要求が到着した場合，すべての処理が終わるまでの時間はタスクの多重度が 1 のときと 2 のときとで，何秒の差があるか。

ア　6　　イ　7　　ウ　8　　エ　9

問10　システムの性能向上策の適用に関して，次の式から導くことができるものはどれか。

$$P=\frac{1}{(1-a)+\frac{a}{V}}$$

ここで，Pはシステムの性能向上率，Vはその性能向上策の性能向上率，aはその性能向上策が及ぶ範囲の全体に対する比率とする。

ア　幾つかの性能向上策を組み合わせて，相乗効果を出すべきである。

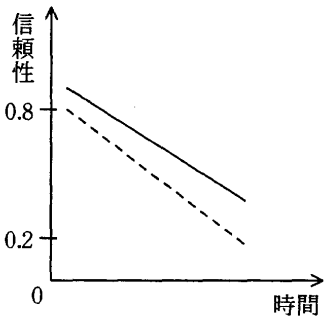
イ　性能向上策が及ぶ範囲の比率が一定で変化しない性能向上策を適用すべきである。

ウ　性能面のボトルネック要因を解消する性能向上策を適用すべきである。

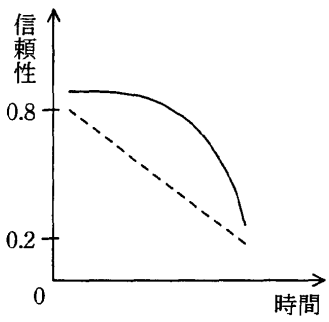
エ　できる限り多くの性能向上策を適用すべきである。

問11　3 個の構成要素のうち 2 個以上が正常ならば正しい結果が得られるようなシステムにおいて，個々の構成要素の信頼性が時間の経過とともに破線のグラフで示すように低下する場合，システム全体の信頼性の変化の傾向を表す実線のグラフとして適切なものはどれか。

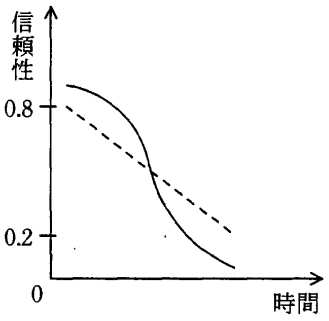
ア



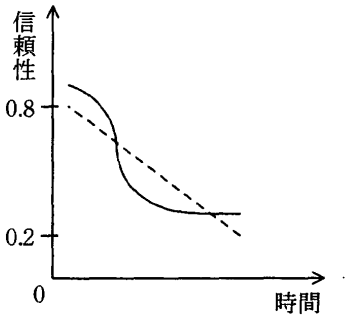
イ



ウ



エ



問12　あるシステムでは，平均すると 100 時間に 2 回の故障が発生し，その都度復旧に 2 時間を要していた。機器を交換することによって，故障の発生が 100 時間で 1 回になり，復旧に要する時間も 1 時間に短縮した。機器を交換することによって，このシステムの稼働率は幾ら向上したか。

ア　0.01　　イ　0.02　　ウ　0.03　　エ　0.04

問13 フェールソフトの説明として，適切なものはどれか。

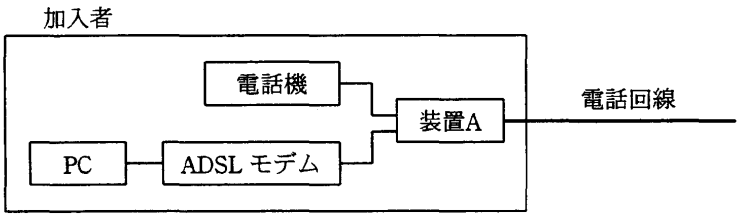
ア　システムの一部に障害が発生したとき，それ以外の部分の機能でシステムの運転を継続する。

イ　システムの一部に障害が発生したとき，致命的影響を与えないよう，システムをあらかじめ定めた安全な状態に移行する。

ウ　信頼度の高い部品を使用したり，バグの少ないソフトウェアを開発したりして，信頼性の高いシステムを構築する。

エ　特定の時点でデータベースのバックアップを取り，障害が発生した場合には，バックアップを取った時点の状態まで戻して運転を継続する。

問14 既存の電話回線を利用した ADSL サービスで，ADSL モデムと電話機を接続する装置 A はどれか。



ア　スプリッタ　　イ　ターミナルアダプタ

ウ　ダイヤルアップルータ　　エ　ハブ

問15 データマイニングの説明として，適切なものはどれか。

ア　大量のデータを高速に検索するための並行的アクセス手法

イ　大量のデータを統計的，数学的な手法で分析し，法則や因果関係を引き出す技術

ウ　販売実績などの時系列データを大量に蓄積したデータベースの保存手法

エ　ユーザの利用目的に合わせて，部門別のデータベースを作成する技術

問16 CMMI を説明したものはどれか。

ア　ソフトウェア開発組織及びプロジェクトのプロセスの成熟度を評価するためのモデルである。

イ　ソフトウェア開発のプロセスモデルの一種である。

ウ　ソフトウェアを中心としたシステム開発及び取引のための共通フレームのことである。

エ　プロジェクトの成熟度に応じてソフトウェア開発の手順を定義したモデルである。

問17 UML を DFD 又は E-R 図と対比した記述のうち，適切なものはどれか。

ア　UML ではデータの関係を記述できないので，E-R 図を併用する必要がある。

イ　UML ではデータの流れを記述できないので，DFD を併用する必要がある。

ウ　UML におけるコラボレーション図（協調図）やコンポーネント図が DFD に相当する。

エ　UML における静的な構造を示すクラス図が，E-R 図に相当する。

問18 モジュール設計に関する記述のうち，モジュール強度が最も高いものはどれか。

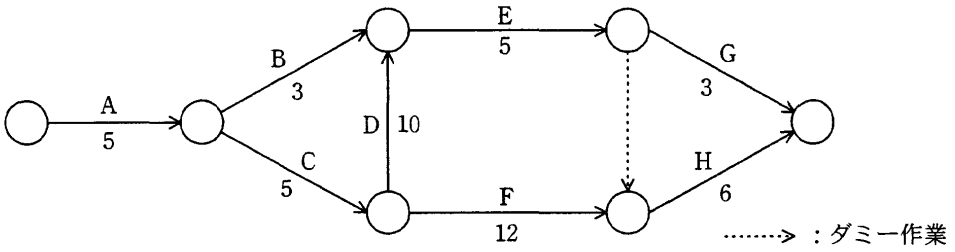
ア　ある木構造データを扱う機能をデータとともに一つにまとめ，木構造データをモジュールの外から見えないようにした。

イ　複数の機能のそれぞれに必要な初期設定の操作が，ある時点で一括して実行できるので，一つのモジュールにまとめた。

ウ　二つの機能 A，B のコードは重複する部分が多いので，A，B を一つのモジュールとし，A，B の機能を使い分けるための引数を設けた。

エ　二つの機能 A，B は必ず A，B の順番に実行され，しかも A で計算した結果を B で使うことがあるので，一つのモジュールにまとめた。

問19　次のアローダイアグラムで表される作業 A～H を見直したところ，作業 D だけが短縮可能であり，その所要日数を 6 日間にできることが分かった。業務全体の所要日数は何日間短縮できるか。ここで，矢印に示す数字は各作業の所要日数を表す。



ア　1　　イ　2　　ウ　3　　エ　4

問20　ファイル障害時の復旧手順を確立するための検討項目の順番として，適切なものはどれか。

a.　各業務，ファイル別の，使用不能となった原因ごとのリカバリ手順のマニュアル化

b.　業務の重要度に応じた，バックアップの取得方法，取得サイクル，バックアップファイルの保管場所などの決定

c.　ファイルが使用不能となった原因ごとのシステム復旧に要する時間の設定

d.　ファイルが使用不能となる原因の分類と，それらの原因による使用不能事態の発生から復元までに許される時間の基準の設定

ア　b, c, d, a　　イ　b, d, a, c

ウ　d, b, c, a　　エ　d, c, a, b

問21　システムの一斉移行方式の特徴はどれか。

ア　運用方法はシステム稼働後に段階的に周知されるので，利用者の混乱が避けられる。

イ　システム規模が小さい場合に行われ，移行に失敗した場合の影響範囲を限定することができる。

ウ　新旧システムを並行して運用することによる作業の二重負担を避けることができ，経済的効果が大きい。

エ　新システムの処理結果と従来システムの処理結果を比較しながら運用することができ，問題がなければ比較作業を一斉にやめて新システムに移行できる。

問22　運用しやすいシステム作りや，本稼働へのスムーズな移行のために，運用部門が果たすべき役割として，適切なものはどれか。

ア　システム開発部門が作成したジョブ構成を変更せずに管理する。

イ　システム開発部門が作成した本稼働への移行手順を利用部門に周知徹底する。

ウ　システム開発部門の開発スケジュールを優先して本稼働までの日程計画を立てる。

エ　システムの設計段階からプロジェクトに参加して運用ドキュメントの標準化を進める。

問23　多重プログラミングを行っているシステムで，システム全体のスループット低下を招くようなプログラムの組合せはどれか。

ア　演算処理が中心となるプログラム同士

イ　共有データを格納したメモリ領域を参照するプログラム同士

ウ　異なる磁気ディスクにアクセスするプログラム同士

エ　利用者の入力操作と入力されたデータの演算処理とが混在しているプログラム同士

問24　雷サージによって通信回線に誘起された異常電圧から通信機器を防護するための装置はどれか。

ア　IDF（intermediate distributing frame）
イ　MDF（main distributing frame）
ウ　アレスタ
エ　避雷針

問25　次の作業を必要とする計画はどれか。

・要員計画の作成
・運用ドキュメントの点検
・運用体制の整備
・データ量の調査・確認（トランザクション件数，最繁時トラフィックの調査・確認）
・設備負荷の調査

ア　システム移行計画　　イ　システム開発計画
ウ　システム監査計画　　エ　システム保守計画

問26　システム運用部門がCPU利用率，ページフォールト頻度などを測定したところ，スラッシングの発生が多くなっていることが分かった。処理能力を改善するために運用部門だけでできる当面の対応処置として，適切なものはどれか。

ア　磁気ディスクの作業域（ワークエリア）の割当てを変更する。
イ　ジョブの多重度を下げて，メモリの使用を抑制する。
ウ　ページ置換方式を変更する。
エ　補助記憶装置を増設して，作業域を再配置する。

問27　運用管理を行う上で，業務システムとそのクライアントとを対応付けておくことによって，システム障害時に可能となるものはどれか。

ア　影響範囲の把握
イ　回避策の立案
ウ　業務処理能力の低下度合いの把握
エ　復旧手順情報の蓄積

問28　ツールレス保守に該当するものはどれか。

ア　異常が発生した場合，現場から離れた保守センタから障害状況を調査する。
イ　故障の前兆となる現象を事前にとらえて，対象となる部品を取り替える。
ウ　サーバマシン内部の基板などをモジュール化し，取付けをレバー式にする。
エ　電源や磁気ディスクなどを二重化し，故障時は縮退運転して故障装置を交換する。

問29　既存のプログラムやファイルを解析して仕様書を作成し，これを参考にして同等の機能をもったプログラムやファイルを作成する開発手法はどれか。

ア　コンカレントエンジニアリング　　イ　リエンジニアリング
ウ　リバースエンジニアリング　　エ　リユーステクノロジ

問30　ソフトウェアの保守管理において，保守作業の生産性に**影響しないもの**はどれか。

ア　運用中に発生するソフトウェアの障害件数
イ　ソフトウェアの検証を行うときの難易度
ウ　ソフトウェアを変更するときの難易度
エ　プログラムやドキュメントの理解しやすさの度合い

問31 IPv4 の IP アドレスに関する記述のうち，適切なものはどれか。

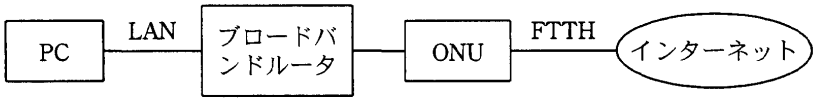
ア　IP アドレスのクラス分けは，32 ビットのうちの先頭 2 ビットによって，クラス A からクラス D までの四つのクラスに識別される。

イ　IP アドレスは 32 ビットであり，8 ビットごとに四つの部分に分けて，16 進数で表記する。

ウ　IP アドレスは 32 ビットであり，クラス A，クラス B 及びクラス C のアドレスフィールドは，ネットワークアドレス部とホストアドレス部とに分かれる。

エ　限られた IP アドレス空間を有効に利用するために，32 ビットのうちのネットワークアドレス部を分割して一部をサブネットアドレス部として使用する。

問32 100 M ビット／秒の LAN に接続されているブロードバンドルータ経由でインターネットを利用している。FTTH の実効速度が 90 M ビット／秒で，LAN の伝送効率が 80％のときに，LAN に接続された PC でインターネット上の 540 M バイトのファイルをダウンロードするのにかかる時間は，およそ何秒か。ここで，制御情報やブロードバンドルータの遅延時間などは考えず，また，インターネットは十分に高速であるものとする。



ア　43　　イ　48　　ウ　54　　エ　60

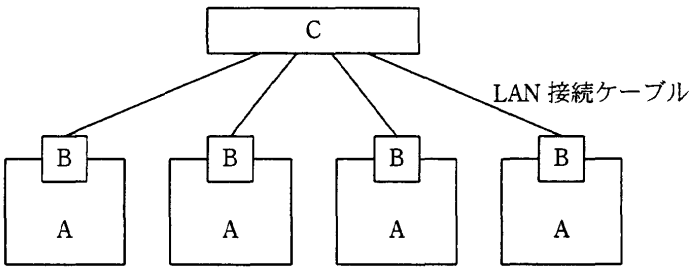
問33　LAN のアクセス制御方式である CSMA/CD 方式に関する説明として，適切なものはどれか。

ア　送出した信号の衝突を検知した場合は，ランダムな時間の経過後に再送信する。
イ　送信権を与えるメッセージ（フリートークン）を得たノードがデータを送信する。
ウ　ディジタル信号をアナログ信号に変換（変調）して通信を行う。
エ　転送する情報を，セルと呼ばれる固定長のブロックに分割して転送する。

問34　磁気ディスク装置や磁気テープ装置などのストレージ（補助記憶装置）を，通常の LAN とは別の高速な専用ネットワークで構成する方式はどれか。

ア　DAFS　　イ　DAS　　ウ　NAS　　エ　SAN

問35　図は 10BASE-T による LAN 接続ケーブルを用いて，PC を接続したネットワークの概念図である。図中の A を PC，B をネットワークインタフェースカードとしたとき，C の装置名として適切なものはどれか。



ア　ターミネータ　　イ　トランシーバ
ウ　ハブ　　エ　モデム

問36 関係データベースとオブジェクト指向データベースを比較したとき，オブジェクト指向データベースの特徴として，適切なものはどれか。

ア　実世界の情報をモデル化したクラス階層を表現でき，このクラス階層を使うことによって，データと操作を分離して扱うことができる。

イ　データと手続がカプセル化され一体として扱われるので，構造的に複雑で，動作を含む対象を扱うことができる。

ウ　データの操作とリレーションが数学的に定義されており，プログラム言語とデータ操作言語との独立性を保つことができる。

エ　リレーションが論理的なデータ構造として定義されており，非手続的な操作言語でデータ操作を行うことができる。

問37 E-R 図に関する記述として，適切なものはどれか。

ア　関係データベースへの実装を前提に作成する。

イ　業務上の各プロセスとデータの関係を明らかにする。結果として導かれる実体間の関連は，業務上の各プロセスを表現する。

ウ　業務で扱う情報を抽象化し，実体及び実体間の関連を表現する。

エ　データの生成から消滅に至るプロセスを表現する。

問38 更新可能なビューを作成するSQL文はどれか。ここで，SQL文中に現れる表はすべて更新可能とする。

ア
```
CREATE VIEW 高額商品(商品番号, 商品名)
AS SELECT 商品番号, 商品名 FROM 商品 WHERE 商品単価 > 1000
```

イ
```
CREATE VIEW 商品受注(商品番号, 受注数量)
AS SELECT 商品番号, SUM(受注数量) FROM 受注 GROUP BY 商品番号
```

ウ
```
CREATE VIEW 受注一覧(受注番号, 商品名, 受注数量, 受注金額)
AS SELECT 受注番号, 商品名, 受注数量, 受注数量*受注単価 FROM 受注, 商品
   WHERE 受注.商品番号 = 商品.商品番号
```

エ
```
CREATE VIEW 受注商品(商品番号)
AS SELECT DISTINCT 商品番号 FROM 受注
```

問39　二つの表 S と SP から部品番号 P2 の部品を納入している納入業者名を探す SQL 文はどれか。ここで，下線部は主キーを表す。

S

納入業者番号	納入業者名	住所

SP

納入業者番号	部品番号	納入量

ア
```
SELECT 納入業者名 FROM S, SP
    WHERE S.納入業者番号 = SP.納入業者番号
```

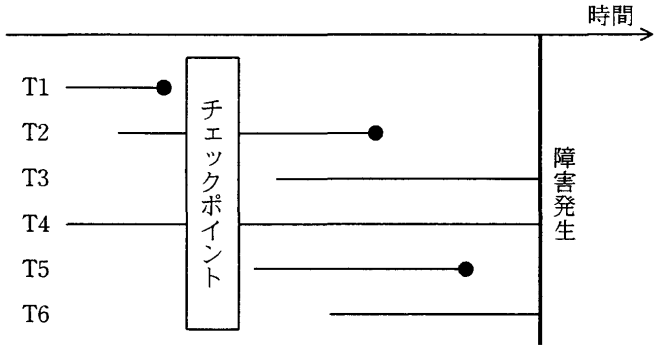
イ
```
SELECT 納入業者名 FROM S
    WHERE 納入業者番号
        IN (SELECT 納入業者番号 FROM SP WHERE 部品番号 = 'P2')
```

ウ
```
SELECT 納入業者名 FROM S
    WHERE NOT EXISTS
        (SELECT * FROM SP
            WHERE 納入業者番号 = S.納入業者番号 AND 部品番号 = 'P2')
```

エ
```
SELECT 納入業者名 FROM S
    WHERE EXISTS
        (SELECT * FROM SP
            WHERE 納入業者番号 = S.納入業者番号 AND 部品番号 > 'P2')
```

問40　DBMS を障害発生後に再立上げするとき，前進復帰（ロールフォワード）すべきトランザクションと後退復帰（ロールバック）すべきトランザクションの組合せとして，適切なものはどれか。ここで，トランザクションの中で実行される処理内容は次のとおりとする。

トランザクション	データベースに対する Read 回数 と Write 回数
T1，T2	Read 10，Write 20
T3，T4	Read 100
T5，T6	Read 20，Write 10



——— はコミットされていないトランザクションを示す。
———● はコミットされたトランザクションを示す。

	前進復帰	後退復帰
ア	T2，T5	T6
イ	T2，T5	T3，T6
ウ	T1，T2，T5	T6
エ	T1，T2，T5	T3，T6

問41 公開鍵暗号方式に関する記述のうち，適切なものはどれか。

ア AESは，NISTが公募し，1997年に決定した公開鍵暗号方式の一種である。

イ RSAは，素因数分解の計算の困難さを利用した，公開鍵暗号方式の一種である。

ウ 公開鍵暗号方式の難点は，鍵の管理が煩雑になることである。

エ 通信文の内容の秘匿に公開鍵暗号方式を使用する場合は，受信者の復号鍵を公開する。

問42 ディジタル署名を利用する目的はどれか。

ア 受信者が署名用の鍵を使って暗号文を元の平文に戻すことができるようにする。

イ 送信者が署名用の鍵を使って作成した署名を平文に付加することによって，受信者が送信者を確認できるようにする。

ウ 送信者が署名用の鍵を使って平文を暗号化し，平文の内容を関係者以外に分からないようにする。

エ 送信者が定数を付加した平文を署名用の鍵を使って暗号化し，受信者が復号した定数を確認することによって，メッセージの改ざん部位を特定できるようにする。

問43 JPCERT/CC（JPCERT コーディネーションセンター）では，インシデントを六つのタイプに分類している。

Scan： プローブ，スキャン，そのほかの不審なアクセス

Abuse： サーバプログラムの機能を悪用した不正中継

Forged： 送信ヘッダを詐称した電子メールの配送

Intrusion： システムへの侵入

DoS： サービス運用妨害につながる攻撃

Other： その他

次の三つのインシデントに対するタイプの組合せのうち，適切なものはどれか。

インシデント1：ワームの攻撃が試みられた形跡があるが，侵入されていない。

インシデント2：ネットワークの輻輳（ふくそう）による妨害を受けた。

インシデント3：DoS用の踏み台プログラムがシステムに設置されていた。

	インシデント1	インシデント2	インシデント3
ア	Abuse	DoS	Intrusion
イ	Abuse	Forged	DoS
ウ	Scan	DoS	Intrusion
エ	Scan	Forged	DoS

問44 認証局（CA）に登録されている通信相手の公開鍵を使用して行えることはどれか。

ア CAから証明書の発行を受ける。

イ 受信した暗号文を復号する。

ウ ディジタル署名を検証する。

エ メッセージにディジタル署名をする。

問45 IDS（Intrusion Detection System）の特徴のうち，適切なものはどれか。

ア　ネットワーク型 IDS では，SSL を利用したアプリケーションを介して行われる攻撃を検知できる。

イ　ネットワーク型 IDS では，通信内容の解析によって，ファイルの改ざんを検知できる。

ウ　ホスト型 IDS では，シグネチャとのパターンマッチングを失敗させるためのパケットが挿入された攻撃でも検知できる。

エ　ホスト型 IDS では，到着する不正パケットの解析によって，ネットワークセグメント上の不正パケットを検知できる。

問46 クロスサイトスクリプティングに該当するものはどれか。

ア　悪意をもったスクリプトを，標的となるサイト経由でユーザのブラウザに送り込み，その標的にアクセスしたユーザのクッキーにある個人情報を盗み取る。

イ　クラッカの Web サイトにアクセスしたユーザに悪意をもったスクリプトを送り込み，そのスクリプトを実行させて Web ページ中の HTML タグを変換する。

ウ　攻撃者が，JavaScript を使ったセッション管理に使うクッキーにアクセスし，ブラウザに広告などのダミー画面を表示する。

エ　入力情報を確認するためにフォームの入力値を画面表示するプログラムの脆弱性を利用して，クッキーにある個人情報を改ざんする。

問47 ステガノグラフィの機能はどれか。

ア　画像データなどにメッセージを埋め込み，メッセージの存在そのものを隠す。

イ　メッセージの改ざん，なりすましの検出，及び否認防止を行う。

ウ　メッセージの認証を行って改ざんの有無を検出する。

エ　メッセージを決まった手順で変換し，通信途中での盗聴を防ぐ。

問48 送信者がメッセージからブロック暗号（方式）を用いて生成したメッセージ認証符号（MAC: message authentication code）をメッセージとともに送り，受信者が受け取ったメッセージからMACを生成して，送られてきたMACと一致することを確認するメッセージ認証で使用される鍵の組合せはどれか。

	送信者	受信者
ア	受信者と共有している共通鍵	送信者と共有している共通鍵
イ	受信者の公開鍵	受信者の秘密鍵
ウ	送信者の公開鍵	受信者の秘密鍵
エ	送信者の秘密鍵	受信者の公開鍵

問49 情報システムへの脅威とセキュリティ対策の組合せのうち，適切なものはどれか。

	脅威	セキュリティ対策
ア	地震と火災	フォールトトレラント方式のコンピュータによるシステムの二重化
イ	データの物理的な盗難と破壊	ディスクアレイやファイアウォール
ウ	伝送中のデータへの不正アクセス	HDLCプロトコルのCRC
エ	メッセージの改ざん	公開鍵暗号方式を応用したディジタル署名

問50 SSL の利用に関する記述のうち，適切なものはどれか。

ア　SSL で使用する個人認証用のディジタル証明書は，IC カードなどに格納できるので，格納場所を特定の PC に限定する必要はない。

イ　SSL は特定利用者間の通信のために開発されたプロトコルであり，事前の利用者登録が不可欠である。

ウ　ディジタル証明書には IP アドレスが組み込まれているので，SSL を利用する Web サーバの IP アドレスを変更する場合は，ディジタル証明書を再度取得する必要がある。

エ　日本国内では，SSL で使用する共通鍵の長さは，128 ビット未満に制限されている。

問51 情報セキュリティ基本方針文書の取扱いについて，ISMS 認証基準に定められているものはどれか。

ア　一度決めた内容は変更せず，セキュリティ事故発生時に見直す。

イ　機密情報であるので関連する管理者にだけ内容を教育する。

ウ　経営陣によって承認され，全従業員に公表し通知する。

エ　作成したメンバ自身で実施状況を点検する。

問52 コンピュータフォレンジクスを説明したものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。

イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。

ウ　証拠となりうるデータを保全し，その後の訴訟などに備える。

エ　ネットワークの管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。

問53 JIS Q 9001（ISO 9001）に規定されているものはどれか。

ア　外部から購入したソフトウェア製品を最終製品に組み込む場合は，動作検査を実施した後に行う。

イ　設計の妥当性確認は，ソフトウェア開発者自身が行うテスト及びデバッグによって実現される設計検証の一つとして実施する。

ウ　トレーサビリティが要求される製品は，製造番号などによって固有の識別を管理し記録する。

エ　納入製品に組み込むために提供された顧客の所有物には，顧客の知的所有権は含まれない。

問54 国際標準化の動向に関する記述のうち，適切なものはどれか。

ア　“情報技術－情報セキュリティマネジメントの実践のための規範”を規定しているISO/IEC 17799は，JIS X 5080の基になっている。

イ　“品質及び／又は環境マネジメントシステム監査のための指針”を規定しているISO 19011は，システム監査基準の基になっている。

ウ　“品質システム－設計・開発・製造における品質保証モデル”を規定しているISO 9001は，共通フレーム98（SLCP-JCF98）の基になっている。

エ　“プロジェクトマネジメントにおける品質の指針”を規定しているISO 10006は，PMBOKの基になっている。

問55 コンピュータで使われている文字符号の説明のうち，適切なものはどれか。

ア　ASCII 符号はアルファベット，数字，特殊文字及び制御文字からなり，漢字に関する規定はない。

イ　EUC は文字符号の世界標準を作成しようとして考案された 16 ビット以上の符号体系であり，漢字に関する規定はない。

ウ　Unicode は文字の 1 バイト目で漢字かどうかが分かるようにする目的で制定され，漢字と ASCII 符号を混在可能にした符号体系である。

エ　シフト JIS 符号は UNIX における多言語対応の一環として制定され，ISO として標準化されている。

〔 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 ● 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。