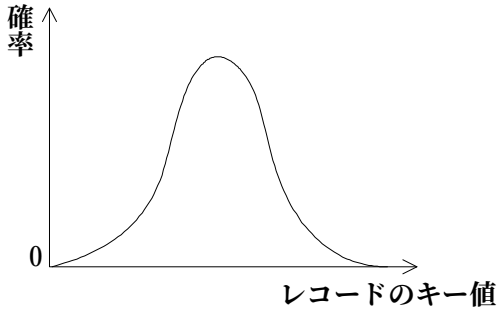
平成１８年度　春期　テクニカルエンジニア（情報セキュリティ）　午前問題

問１　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。

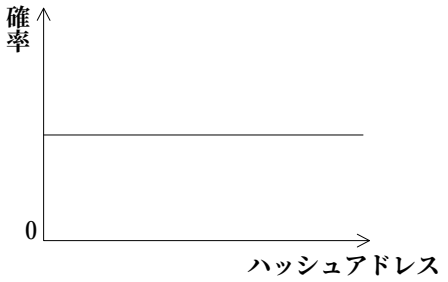
〔ページフォールト発生時の処理時間〕
(1) ページアウトを伴わない場合，ページインの処理で 20 ミリ秒かかる。
(2) ページアウトを伴う場合，置換えページの選択，ページアウト，ページインの処理で合計 60 ミリ秒かかる。

ア　0.25　　イ　0.33　　ウ　0.67　　エ　0.75

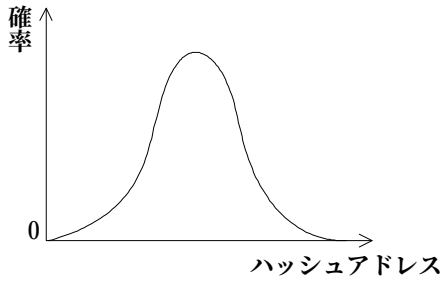
問２　ハッシュ法によるデータ編成法において，レコードのキー値が図のような分布に従って発生する場合，シノニムの発生を最少とするハッシュアドレス（ハッシュした結果のアドレス値）の分布として，適切なものはどれか。



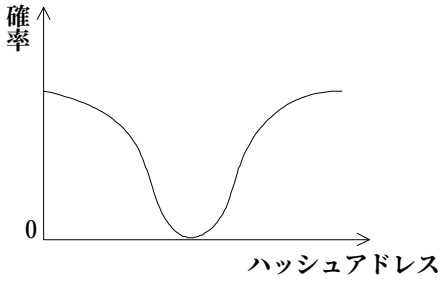
ア



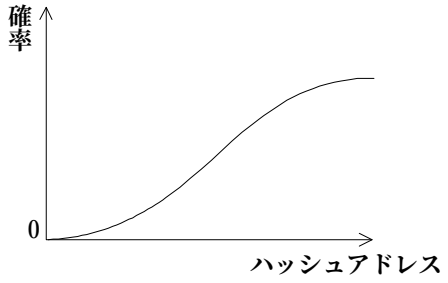
イ



ウ



エ



問３　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。

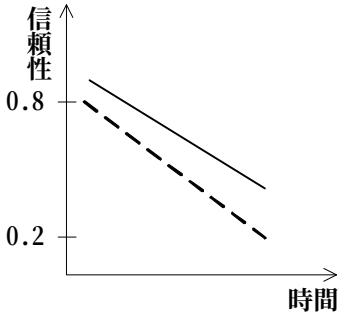
イ　プレゼンテーション層，ファンクション層，データ層に分離したアーキテクチャであり，各層の OS は異なってもよい。

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。

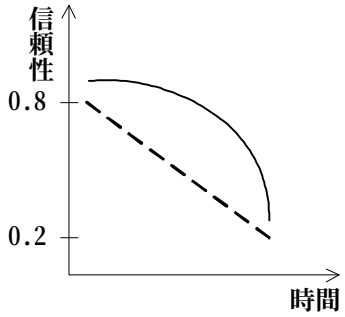
エ　プレゼンテーション層とファンクション層を結合し，データ層を分離したアーキテクチャであり，データベースサーバを効率的に運用できる。

問４　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。

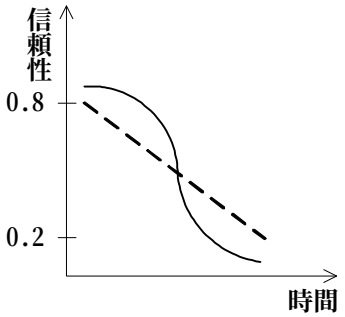
ア



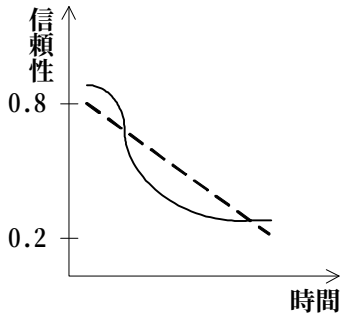
イ



ウ



エ



問５　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６　最初にシステム全体の要求定義を行い，要求された機能を幾つかに分割して段階的にリリースするので，すべての機能がそろっていなくても，最初のリリースからシステムの動作を確認することができるプロセスモデルはどれか。

ア　インクリメンタルモデル　　イ　ウォータフォールモデル

ウ　エボリューショナルモデル　　エ　スパイラルモデル

問７　食品卸業のA社は，インターネット経由で複数の取引先から注文を受け付ける食材受注システムを開発している。取引先によって注文する商品は異なるが，各取引先が注文する品目の日々の変更は少ない。取引先が短時間で商品を指定できると同時に，品目の変更にも即応できる方法として，最も適切なものはどれか。

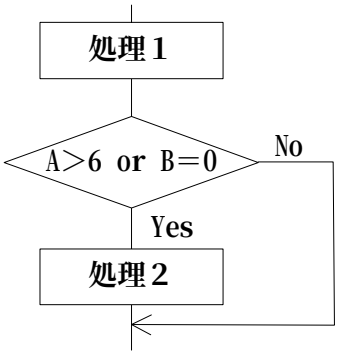
ア　取引先が，A社から配布された商品コード表を見て，商品コードを直接入力する。

イ　取引先が，あらかじめA社にカスタマイズしてもらった商品一覧を表示し，その中から商品を選択する。

ウ　取引先が，商品名や品種分類などで検索することによって商品一覧を表示し，その中から商品を選択する。

エ　取引先が，必要に応じて自分でカスタマイズした商品一覧を表示し，その中から商品を選択する。

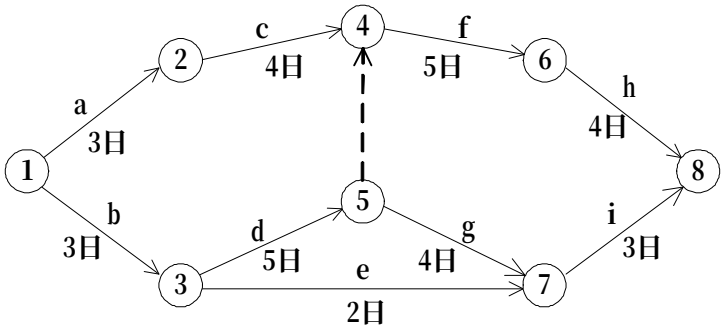
問８　あるプログラムについて，流れ図で示される部分に関するテストデータを，判定条件網羅（分岐網羅）によって設定した。このテストデータを，複数条件網羅による設定に変更したとき，加えるべきテストデータとして，適切なものはどれか。ここで，(　)で囲んだ部分は，一組のテストデータを表すものとする。



・判定条件網羅（分岐網羅）によるテストデータ
(A=4，B=1)，(A=5，B=0)

	加えるべきテストデータ
ア	(A=3，B=0)，(A=7，B=2)
イ	(A=3，B=2)，(A=8，B=0)
ウ	(A=4，B=0)，(A=8，B=0)
エ	(A=7，B=0)，(A=8，B=2)

問９　次のアローダイアグラムを基にして要員計画を立てる。要員数の増減を極力抑え，かつ最短日数で終えられるように計画を立てる場合，1 日当たりの最大要員数は何名になるか。ここで，各工程は 1 名で作業するものとする。



－－－→：ダミー作業

ア　2　　イ　3　　ウ　4　　エ　5

問 10　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 11　ソフトウェアライフサイクルの保守プロセスにおけるアクティビティの一つである保守レビューの目的はどれか。

ア　修正されたシステムの完全性の確認

イ　修正によって影響を受けるインタフェース要素の識別

ウ　発生した障害に対する回避策の有無の判定

エ　保守費用の見積り

問 12　ある企業が専用線を使ってインターネットに接続するとき，インターネットでのホストの識別方法とその企業の IP アドレスの決め方に関する記述のうち，適切なものはどれか。

ア　相手との通信は IP アドレスと MAC アドレスの双方を用いて行われる。MAC アドレスはインターネットサービスプロバイダ(ISP)から取得し，IP アドレスは企業内のアドレスとして任意に決定できる。

イ　相手との通信は IP アドレスを用いて行われるので，一意に付番する必要がある。したがって，ISP に申請して，IP アドレスを事前に取得する必要がある。

ウ　相手との通信は IP アドレスを用いて行われるので，一意に付番する必要がある。したがって，まず自社内で一意になるように IP アドレスを決定してから，ISP に申請し，それが世界中で重複がないかどうかを調査してもらう必要がある。

エ　相手との通信は MAC アドレスだけで行われるので，IP アドレスが重複しても構わない。IP アドレスは，MAC アドレスを分かりやすい名称に読み替えるために使用されるだけなので，任意に決定できる。

問 13　OSPF に関する記述のうち，適切なものはどれか。

ア　経路選択方式は，エリアの概念を取り入れたリンク状態方式である。

イ　異なる管理ポリシが適用された領域間の，エクステリアゲートウェイプロトコルである。

ウ　ネットワークの運用状態に応じて動的にルートを変更することはできない。

エ　隣接ノード間の負荷に基づくルーティングプロトコルであり，コストについては考慮されない。

問 14　TCP ヘッダに含まれる情報はどれか。

ア　あて先ポート番号　　イ　パケット生存時間(TTL)

ウ　発信元 IP アドレス　　エ　プロトコル番号

問 15　IP アドレスが 172.20.100.52/26 のときのサブネットマスクはどれか。

ア　255.255.255.0　　イ　255.255.255.64

ウ　255.255.255.128　　エ　255.255.255.192

問 16　電子メールシステムにおいて，利用者端末がサーバから電子メールを受信するために使用するプロトコルで，選択したメールだけを利用者端末へ転送する機能，サーバ上のメールを検索する機能，メールのヘッダだけを取り出す機能などをもつものはどれか。

ア　IMAP4　　イ　MIME　　ウ　POP3　　エ　SMTP

問 17　シリアル回線で使用するデータリンクのコネクション確立やデータ転送を，LAN 上で実現するプロトコルはどれか。

ア　MPLS　　イ　PPP　　ウ　PPPoE　　エ　PPTP

問 18　インターネットで電子メールを送信するとき，メッセージの本文の暗号化に共通鍵暗号方式を用い，共通鍵の受渡しには公開鍵暗号方式を用いるものはどれか。

ア　AES　　イ　IPsec　　ウ　MIME　　エ　S/MIME

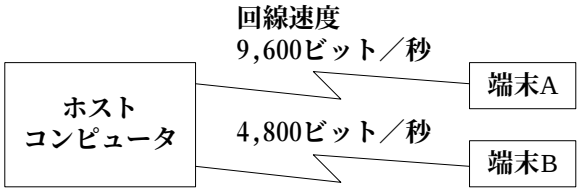
問 19　IEEE 802.3 は，CSMA/CD 方式による LAN のアクセス方式の標準である。OSI 基本参照モデルのうち，IEEE 802.3 で規定されている最上位層はどれか。

ア　セション層　　イ　データリンク層
ウ　トランスポート層　　エ　ネットワーク層

問 20　巡回冗長検査(CRC)の特徴に関する記述のうち，最も適切なものはどれか。

ア　生成多項式が n 次の場合，長さ n 以下のバースト誤りをすべて検出できる。
イ　メッセージのビット数よりも多くの検査ビットを付加する必要がある。
ウ　メッセージビットに検査ビットを加算したものを，データとして送信する。
エ　文字単位でデータ誤りを検出する方法である。

問 21　図のようなネットワーク構成のシステムにおいて，同じメッセージ長のデータをホストコンピュータとの間で送受信した場合のターンアラウンドタイムは，端末 A では 450 ミリ秒，端末 B では 700 ミリ秒であった。上り，下りのメッセージ長は同じ長さで，ホストコンピュータでの処理時間は端末 A，端末 B のどちらから利用しても同じとするとき，端末 B からホストコンピュータへの片道の伝送時間は何ミリ秒か。ここで，ターンアラウンドタイムは，端末がデータを回線に送信し始めてから応答データを受信し終わるまでの時間とし，伝送時間は回線速度だけに依存するものとする。



ア　100　　イ　150　　ウ　200　　エ　250

問 22　LAN のノード（制御装置，端末など）を接続する配線の形態に関する記述のうち，バス形配線に該当するものはどれか。

ア　ケーブルを環状に敷設し，そこに全ノードが接続されている。

イ　中央に制御用のノードを配置し，そこに全ノードが接続されている。

ウ　中央のノードに幾つかのノードが接続され，それらから更に別のノードが接続されている。

エ　同軸ケーブルなどの 1 本のケーブルに，全ノードが接続されている。

問 23　IPsec に関する記述のうち，適切なものはどれか。

ア　IKE は IPsec の鍵交換のためのプロトコルであり，ポート番号 80 が使用される。

イ　鍵交換プロトコルとして，HMAC-MD5 が使用される。

ウ　トンネルモードで暗号化を使用すると，元のヘッダまで含めて暗号化される。

エ　ホスト A とホスト B との間で IPsec による通信を行う場合，認証や暗号化アルゴリズムを両者で決めるために ESP ヘッダではなく AH ヘッダを使用する。

問 24　ITU-T 勧告 H.323 で規定されているインターネット電話のゲートキーパの機能として，適切なものはどれか。

ア　音声の品質を確保するために，パケットを一時的に蓄積し，音声の復号を行う。

イ　音声の符号化，圧縮を行う。

ウ　回線交換網と LAN を接続するために，インタフェースを変換する。

エ　システム内の端末の登録，帯域幅の割当て，端末アドレスの管理などを行う。

問 25　ネットワーク管理プロトコルである SNMP のメッセージタイプのうち，異常や事象の発生をエージェントからマネージャに知らせるために使用するものはどれか。

ア　get-request　　イ　get-response　　ウ　set-request　　エ　trap

問 26　ネットワークの制御に関する記述のうち，適切なものはどれか。

ア　TCP では，ウィンドウサイズが固定で輻輳回避ができないので，輻輳が起きると，データに対してタイムアウト処理が必要になる。

イ　誤り制御方式の一つであるフォワード誤り訂正方式は，受信側で誤りを検出し，送信側にデータの再送を要求する方式である。

ウ　ウィンドウによるフロー制御では，応答確認のあったブロック数だけウィンドウをずらすことによって，複数のデータをまとめて送ることができる。

エ　データグラム方式では，両端を結ぶ仮想の通信路を確立し，以降はすべてその経路を通すことによって，経路選択のオーバヘッドを小さくしている。

問 27　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 28　関係データベースの利用において，仮想の表（ビュー）を作る目的として，適切なものはどれか。

ア　記憶容量を節約するため

イ　処理速度を向上させるため

ウ　セキュリティを向上させるためや表操作を容易にするため

エ　デッドロックの発生を減少させるため

問 29　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 30　“診療科”表，“医師”表及び“患者”表がある。患者がどの医師の診察も受けることができ，かつ医師の特定もできる“診察”表はどれか。ここで，表定義中の実線の下線は主キーを，破線の下線は外部キーを表す。

診療科

診療科コード	診療科名称

医師

医師番号	医師名	診療科コード

患者

患者番号	患者名

ア

医師番号	患者番号	診察日時

イ

医師番号	診察日時

ウ

診療科コード	医師番号	診察日時

エ

診療科コード	患者番号	診察日時

問 31　四つの表“注文”,“顧客”,“商品”,“注文明細”がある。これらの表から，次のビュー“注文一覧”を作成する SQL 文はどれか。ここで，下線の項目は主キーを表す。

注文（注文番号，注文日，顧客番号）
顧客（顧客番号，顧客名）
商品（商品番号，商品名）
注文明細（注文番号，商品番号，数量，単価）

注文一覧

注文番号	注文日	顧客名	商品名	数量	単価
001	2006-01-10	佐藤	AAAA	5	5,000
001	2006-01-10	佐藤	BBBB	3	4,000
002	2006-01-15	田中	BBBB	6	4,000
003	2006-01-20	高橋	AAAA	3	5,000
003	2006-01-20	高橋	CCCC	10	1,000

ア
```
CREATE VIEW 注文一覧
      AS SELECT * FROM 注文,顧客,商品,注文明細
         WHERE    注文.注文番号 = 注文明細.注文番号 AND
                  注文.顧客番号 = 顧客.顧客番号 AND
                  商品.商品番号 = 注文明細.商品番号
```

イ
```
CREATE VIEW 注文一覧
      AS SELECT   注文.注文番号,注文日,顧客名,商品名,数量,単価
         FROM     注文,顧客,商品,注文明細
         WHERE    注文.注文番号 = 注文明細.注文番号 AND
                  注文.顧客番号 = 顧客.顧客番号 AND
                  商品.商品番号 = 注文明細.商品番号
```

ウ
```
CREATE VIEW 注文一覧
      AS SELECT   注文.注文番号,注文日,顧客名,商品名,数量,単価
         FROM     注文,顧客,商品,注文明細
         WHERE    注文.注文番号 = 注文明細.注文番号 OR
                  注文.顧客番号 = 顧客.顧客番号 OR
                  商品.商品番号 = 注文明細.商品番号
```

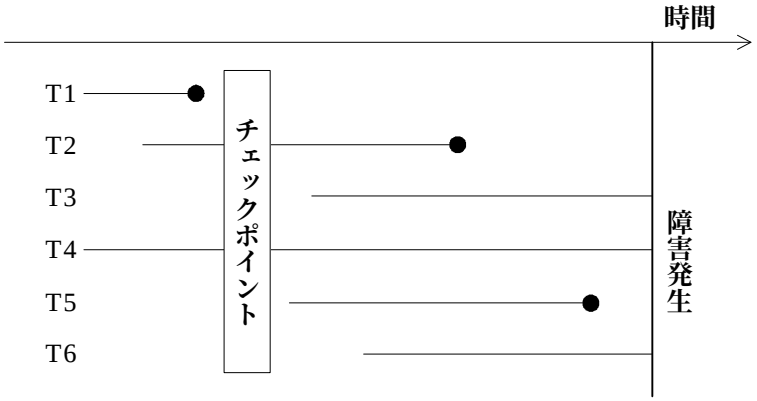
エ
```
CREATE VIEW 注文一覧
      AS SELECT   注文.注文番号,注文日,商品名,数量,単価
         FROM     注文,商品,注文明細
         WHERE    注文.注文番号 = 注文明細.注文番号 AND
                  商品.商品番号 = 注文明細.商品番号
```

問32　トランザクションの並行制御において，変更消失（Lost update）の問題，コミットされていない依存性（uncommitted dependency）の問題，不整合分析（inconsistent analysis）の問題が起こる可能性がある。これらの問題を解決する技術と，この技術を使うことによって新たに発生する問題の組合せはどれか。

	解決する技術	新たに発生する問題
ア	時刻印アルゴリズム	デッドロック
イ	時刻印アルゴリズム	ロックによる待ち
ウ	ロック	更新矛盾
エ	ロック	デッドロック

問 33　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 34　オンライントランザクションの原子性(atomicity)の説明として，適切なものはどれか。

ア　データの物理的格納場所やアプリケーションプログラムの実行場所を意識することなくトランザクション処理が行える。

イ　トランザクションが完了したときの状態は，処理済みか未処理のどちらかしかない。

ウ　トランザクション処理においてデータベースの一貫性が保てる。

エ　複数のトランザクションを同時に処理した場合でも，個々の処理結果は正しい。

問 35　事業本部制をとっている A 社で，社員の所属を管理するデータベースを作成することになった。データベースは表 a，b，c で構成されている。新しいデータを追加するときに，ほかの表でキーになっている列の値が，その表に存在しないとエラーとなる。このデータベースに，各表ごとにデータを入れる場合の順序として，適切なものはどれか。ここで，下線は各表のキーを示す。

表 a	社員番号	氏名	事業本部コード	部門コード

表 b	事業本部コード	事業本部名

表 c	事業本部コード	部門コード	部門名

ア　表 a → 表 b → 表 c　　**イ　表 a → 表 c → 表 b**

ウ　表 b → 表 a → 表 c　　**エ　表 b → 表 c → 表 a**

問 36　電子メールにおけるメッセージダイジェスト（メッセージ認証符号）を説明したものはどれか。

ア　メッセージから，ある規則によってデータをサンプリングし，一定の長さのデータにしたもの

イ　メッセージの暗号化に用いた共通鍵を，受信者の公開鍵で暗号化したもの

ウ　メッセージを，あるアルゴリズムによって一定の長さのデータに変換し，送信者の秘密鍵で暗号化したもの

エ　メッセージを，あるアルゴリズムによって一定の長さのデータに変換したもの

問 37　暗号解読のための攻撃法のうち，ブルートフォース攻撃はどれか。

ア　与えられた平文と暗号文の組に対して鍵を総当たりで探索して解読を試みる。

イ　暗号化関数の統計的な偏りを線形関数によって近似して解読を試みる。

ウ　暗号化装置のソフトウェアやハードウェアの解析を行って解読を試みる。

エ　異なる二つの平文とそれぞれの暗号文の差分を観測して解読を試みる。

問 38　セキュリティ対策で利用するリスト CRL に記載される情報はどれか。

ア　スパムメールの発信元及びメールの不正中継を行うドメインの名前

イ　ディジタル証明書の有効期間内に認証局の廃止などによって失効した自己署名と相互認証の両証明書

ウ　有効期間内に無効となったディジタル証明書のシリアル番号

エ　利用者に対して与えられた情報資源へのアクセス権限

問 39　データ送受信に利用するアルゴリズム SHA-1 を説明したものはどれか。

ア　160 ビットの出力データを生成し，改ざんの検出に利用するアルゴリズム

イ　IPsec で使用される暗号化アルゴリズム

ウ　暗号化鍵を生成するアルゴリズム

エ　データの暗号化が正常に完了したことの確認に利用するアルゴリズム

問 40　フィッシング(phishing)による被害はどれか。

ア　インターネットからソフトウェアをダウンロードしてインストールしたところ，設定したはずのない広告がデスクトップ上に表示されるようになった。

イ　インターネット上の多数のコンピュータから公開しているサーバに一斉にパケットが送り込まれたので，当該サーバが一時使用不能になった。

ウ　知人から送信されてきた電子メールに添付されていたファイルを実行したところ，ハードディスク上に存在するすべてのファイルを消失してしまった。

エ　“本人情報の再確認が必要なので入力してください”という電子メールで示された URL にアクセスし，個人情報を入力したところ，詐取された。

問 41　IP スプーフィング(spoophing)攻撃による，自ネットワークのホストへの侵入を防止するのに有効な対策はどれか。

ア　外部から入る TCP コネクション確立要求パケットのうち，外部へのインターネットサービスの提供に必要なもの以外を阻止する。

イ　外部から入る UDP パケットのうち，外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を阻止する。

ウ　外部から入るパケットが，インターネットとの直接の通信をすべきでない内部ホストの IP アドレスにあてられていれば，そのパケットを阻止する。

エ　外部から入るパケットの発信元 IP アドレスが自ネットワークのものであれば，そのパケットを阻止する。

問 42　フィールド 1 に入力された値が変数 $jouken1 に，フィールド 2 に入力された値が変数 $jouken2 に代入され，次の SQL 文によって表 TABLE_A を検索して結果を表示する Web アプリケーションがある。

```
SELECT * FROM TABLE_A WHERE jouken1 = '$jouken1' AND jouken2 = '$jouken2'
```

悪意のあるユーザが SQL インジェクションによって，TABLE_A の全レコードの削除を試みるとき，それぞれのフィールドに入力する文字列はどれか。

	フィールド 1	フィールド 2
ア	*	'DELETE FROM TABLE_A WHERE 'A'='A
イ	*	DELETE FROM TABLE_A WHERE 'A'='A'
ウ	（何も入力しない）	';DELETE FROM TABLE_A WHERE 'A'='A
エ	（何も入力しない）	DELETE FROM TABLE_A WHERE 'A'='A'

問 43　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 44　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　あらかじめ設定された運用基準に従って送受信するメールを，メールサーバを通過する前にフィルタリングすること

イ　磁気ディスクなどの書換え可能な記憶媒体は単に初期化するだけでは復元される可能性があるので覆い隠すようにデータを上書きすること

ウ　ネットワークやホストに対する外部からの攻撃や侵入を検出し，管理者に通報すること

エ　不正アクセスなどコンピュータに関する犯罪の法的な証拠性を明らかにするために，原因究明に必要な情報を収集して分析すること

問 45　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 46　パケットフィルタリング方式の適用によって実現できるものはどれか。

ア　ftp サービスで転送できるファイルとできないファイルを識別し，制御できる。

イ　通常モードで接続する ftp サービスの使用だけを許可できる。

ウ　特定のポートの通信が通過しない設定をして telnet によるログインを禁止できる。

エ　利用する権限をもっているユーザだけに，telnet サービスの使用を許可できる。

問 47　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 48　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 49　無線 LAN における通信の暗号化の仕組みに関する説明のうち，適切なものはどれか。

ア　EAP は，クライアント PC とアクセスポイントとの間であらかじめ登録した共通鍵による暗号化通信を実現する。

イ　ESS-ID は，クライアント PC ごとの秘密鍵を定めたものであり，公開鍵暗号方式の暗号化通信を実現する。

ウ　IEEE802.1x の規定を利用して，セッションごとに動的に異なる暗号化鍵を用いた暗号化通信を実現する。

エ　WEP は，クライアント PC とアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現する。

問 50　情報システムのセキュリティコントロールを予防，検知，復旧の三つに分けた場合，復旧に該当するものはどれか。

ア　オンラインアクセスにおけるパスワードの利用

イ　コンピュータオペレータとプログラマの職務分離

ウ　コンピュータセンタのコンティンジェンシープラン

エ　メッセージ認証

問 51　リスクファイナンスを説明したものはどれか。

ア　損失の発生率を低下させることによって保険料を節約し，損失の低減を図る。

イ　保険に加入するなど資金面での対策を講じ，リスク移転を図る。

ウ　リスクの原因を除去して保険を掛けずに済ませ，リスク回避を図る。

エ　リスクを扱いやすい単位に分解するか集約することによって保険料を節約し，リスクの分離又は結合を図る。

問 52　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 53　ISO/IEC 15408 の評価対象になるものはどれか。

ア　暗号アルゴリズムの品質

イ　認証局業務の運用受託サービスの管理手順

ウ　パケットフィルタリング機能をもつファイアウォール用ソフトウェア

エ　表示装置からの電磁波放射による情報漏えいの防止方法

問 54　ソフトウェア開発工程を評価・改善するに当たって使用する成熟度モデルはどれか。

ア　CMMI　　イ　MBNQA　　ウ　SLA　　エ　SLCP

問 55　通信用携帯端末（携帯電話）などに動画を配信するときに採用されている圧縮規格はどれか。

ア　JPEG　　イ　MMR　　ウ　MP3　　エ　MPEG4