平成１９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　OS におけるタスクのスケジューリングに関する記述として，適切なものはどれか。

ア　多重待ち行列方式は，タスクに対して最初は低い優先度と長い CPU 時間を割り当て，その後は徐々に優先度を高くし，割り当てる CPU 時間を徐々に短くする方式である。

イ　到着順方式では，タスクが生成された順に高い優先度を付けて CPU 時間を割り当てる。これは先に実行が開始されたタスクを優先させて，早く終了させることを目的としているからである。

ウ　優先度方式では，CPU の利用状況の低いタスクの優先度を順次高くし，逆に CPU を多く利用したタスクの優先度を低くするので，システム全体の処理効率を高めるのに適している。

エ　ラウンドロビン方式は，要求された順番に CPU 時間を割り当て，割り当てられた時間を使い切った後は，待ち行列の末尾に回す方式である。

問２　クライアントサーバシステムにおける，アプリケーション（AP）の処理形態に関する記述として，最も適切なものはどれか。

ア　クライアント側とサーバ側の両方に配置した AP で同期をとりながら多量のデータを処理する形態では，ネットワーク性能よりも，データベース性能を重視する必要がある。

イ　クライアント側に配置した AP で，サーバ側にあるデータを処理する形態は，EUC 重視というよりスループット重視といえる。

ウ　サーバ側に配置した AP とデータを利用して，クライアントから入力したトランザクションを処理する形態は，サーバよりもクライアントに高い処理能力が要求される。

エ　サーバ側に配置した AP をクライアント側に転送して処理し，結果をファイル転送でサーバ側に戻す形態は，サーバとの同期が要求されない処理に適している。

問３　ピアツーピアのデータ探索技術であるフラッディングにおいて，データの所在情報の問合せ先はどれか。

ア　インデックスサーバ

イ　スーパノード群で構成される探索用のネットワーク

ウ　探索するデータのハッシュ値と最も近いハッシュ値をもつインデックスノード

エ　隣接するノード

問４　端末から 400 バイトの電文を送信し，ホストコンピュータが 600 バイトの電文を返信するトランザクション処理システムがある。回線速度を 1×10^6 ビット／秒，回線の伝送効率を 80%，ホストコンピュータのトランザクション当たりの処理時間を 40 ミリ秒とする。ホストコンピュータでの処理待ち時間，伝送制御のための処理時間などは無視できるとした場合，端末における電文の送信開始から受信完了までの時間は何ミリ秒か。ここで，1 バイトは 8 ビットであるものとする。

ア　10　　イ　44　　ウ　46　　エ　50

問５　2 台のプリンタがあり，それぞれの稼働率が 0.7 と 0.6 である。この 2 台のいずれか一方が稼働していて，他方が故障している確率は幾らか。ここで，2 台のプリンタの稼働率は独立に定まり，プリンタ以外の要因は考慮しないものとする。

ア　0. 18　　イ　0. 28　　ウ　0. 42　　エ　0. 46

問６　ソフトウェアをオープンソースソフトウェアとして公開するために OSI（Open Source Initiative）が定めた条件の一つはどれか。

ア　商業的に利用されることを制限している。

イ　特定のソフトウェア配布物に含まれることを条件とすることができる。

ウ　配布の際に機密保持契約を要求している。

エ　派生著作物に元のソフトウェアとは異なる名前やバージョンを付けるように，要請することができる。

問７　安全性や信頼性について，次の方針でプログラム設計を行う場合，その方針を表す用語はどれか。

“不特定多数の人が使用するプログラムには，自分だけが使用するプログラムに比べて，より多くのデータチェックの機能を組み込む。プログラムが処理できるデータの前提条件を文書に書いておくだけでなく，その前提を満たしていないデータが実際に入力されたときは，エラーメッセージを表示して再入力を促すようにプログラムを作る。”

ア　フールプルーフ　　イ　フェールセーフ

ウ　フェールソフト　　エ　フォールトトレラント

問８　工程管理図表に関する記述のうち，ガントチャートの特徴を示すものはどれか。

ア　作業の順序や作業相互の関係を表現したり，重要作業を把握したりするのに適しており，プロジェクトの作業計画などに利用される。

イ　作業の相互関係の把握には適していないが，作業の予定に対する実績を把握するのに適しており，個人やグループの進捗管理に利用される。

ウ　作業の予定と実績を時系列的に表現するのに適しており，将来の予測を立てるときに利用される。

エ　進捗管理上のマイルストーンを把握するのに適しており，プロジェクト全体の進捗管理などに利用される。

問９　JIS X 0129-1 で規定されたソフトウェア製品の品質副特性の説明のうち，信頼性に分類されるものはどれか。

ア　故障時に，指定された達成水準を再確立し，直接に影響を受けたデータを回復するソフトウェア製品の能力

イ　ソフトウェアにある欠陥の診断又は故障原因の追及，及びソフトウェアの修正箇所の識別を行うためのソフトウェア製品の能力

ウ　一つ以上の指定されたシステムと相互作用するソフトウェア製品の能力

エ　利用者がソフトウェアの運用及び運用管理を行うことができるソフトウェア製品の能力

問 10　ITIL におけるサービスサポートのプロセスはどれか。

ア　可用性管理　　イ　キャパシティ管理

ウ　サービスレベル管理　　エ　変更管理

問 11　コンピュータとスイッチングハブ，又は 2 台のスイッチングハブの間を接続する複数の物理回線を論理的に 1 本の回線に束ねる技術はどれか。

ア　スパニングツリー　　イ　ブリッジ

ウ　マルチホーミング　　エ　リンクアグリゲーション

問 12　図は IPsec のデータ形式を示している。ESP トンネルモードの電文中で，暗号化されているのはどの部分か。

新 IP ヘッダ	ESP ヘッダ	オリジナル IP ヘッダ	TCP ヘッダ	データ	ESP トレーラ	ESP 認証データ

ア　ESP ヘッダから ESP トレーラまで

イ　TCP ヘッダから ESP 認証データまで

ウ　オリジナル IP ヘッダから ESP トレーラまで

エ　新 IP ヘッダから ESP 認証データまで

問 13　ネットワークアドレスが 192. 168. 16. 40/29 のとき，適切なものはどれか。

ア　192. 168. 16. 48 は同一サブネットワーク内の IP アドレスである。

イ　サブネットマスクは，255. 255. 255. 240 である。

ウ　使用可能なホストアドレスは最大 6 個である。

エ　ホスト部は 29 ビットである。

問 14　TCP/IP のネットワークにおいて，TCP のコネクションを識別するために必要なものの組合せはどれか。

ア　あて先 IP アドレス，あて先 TCP ポート番号

イ　あて先 IP アドレス，あて先 TCP ポート番号，送信元 IP アドレス，送信元 TCP ポート番号

ウ　あて先 IP アドレス，送信元 IP アドレス

エ　あて先 MAC アドレス，あて先 IP アドレス，あて先 TCP ポート番号，送信元 MAC アドレス，送信元 IP アドレス，送信元 TCP ポート番号

問 15　インターネットプロトコルの TCP と UDP に関するヘッダ情報のうち，TCP のヘッダにだけあるものはどれか。

ア　シーケンス番号　　イ　送信元ポート番号

ウ　チェックサム　　エ　プロトコル番号

問 16　クラス C の IP アドレスを使用し，サブネットに分けたネットワークを構築したい。1 サブネットワーク内の設置ホスト数が最大 64 のとき，適切なサブネットマスクはどれか。

ア　255. 255. 255. 128　　イ　255. 255. 255. 192

ウ　255. 255. 255. 224　　エ　255. 255. 255. 240

問 17　IPv4 のマルチキャストに関する記述のうち，適切なものはどれか。

ア　すべてのマルチキャストアドレスは，あらかじめ用途が固定的に決められている。

イ　マルチキャストアドレスには，クラス D のアドレスが使用される。

ウ　マルチキャストパケットは，ネットワーク上のすべてのコンピュータによって受信され，IP より上位の層で，必要なデータか否かが判断される。

エ　マルチキャストパケットは，ホップ数に関係なく IP マルチキャストルータによって中継される。

問 18　電子メールシステムで使用されるプロトコルである POP3 に関する記述として，適切なものはどれか。

ア　PPP のリンク確立後に，ユーザ ID とパスワードによって利用者を認証するときに使用するプロトコルである。

イ　メールサーバ間でメールメッセージを交換するときに使用するプロトコルである。

ウ　メールサーバのメールボックスからメールを取り出すときに使用するプロトコルである。

エ　ユーザがメールを送るときに使用するプロトコルである。

問 19　RSVP の説明として，適切なものはどれか。

ア　IP ネットワークにおいて，ホスト間通信の伝送帯域を管理するためのプロトコルである。

イ　LAN システムにおいて，物理的なケーブルやノードの接続形態に依存せず，ノードを任意に論理的なグループに分ける技術である。

ウ　PPP によるデータリンクを複数束ねることができるように拡張したプロトコルである。

エ　リモートアクセスを利用するユーザの認証を行うためのプロトコルである。

問 20　符号長 7 ビット，情報ビット数 4 ビットのハミング符号による誤り訂正の方法を，次のとおりとする。

受信した 7 ビットの符号語 $x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$（$x_k = 0$ 又は 1）に対して

$c_0 = x_1 + x_3 + x_5 + x_7$

$c_1 = x_2 + x_3 + x_6 + x_7$

$c_2 = x_4 + x_5 + x_6 + x_7$

（いずれも mod2 での計算）

を計算し，c_0，c_1，c_2 の中に少なくとも一つは 0 でないものがある場合には，

$i = c_0 + c_1 \times 2 + c_2 \times 4$

を求めて，左から i ビット目を反転することによって誤りを訂正する。

受信した符号語が 1000101 であった場合，誤り訂正後の符号語はどれか。

ア　1000001　　イ　1000101　　ウ　1001101　　エ　1010101

問 21　MPEG-1 の説明として，適切なものはどれか。

ア　1.5M ビット／秒程度の圧縮方式であり，主に CD-ROM などの蓄積型メディアを対象にしている。

イ　60M ビット／秒を超える圧縮方式であり，主に高品質なテレビ放送を対象にしている。

ウ　数十 k～数百 k ビット／秒という低ビットレートの圧縮方式の一つであり，携帯電子機器などへの利用を対象にしている。

エ　数 M～数十 M ビット／秒という広い範囲の圧縮方式であり，蓄積型メディア，放送，通信で共通に利用できる汎用の方式である。

問 22　20 台の電話機のトラフィック量を調べたところ，電話機 1 台当たりの呼の発生頻度（発着呼の合計）は 6 分に 1 回，平均回線保留時間は 36 秒であった。このときの呼量は何アーランか。

ア　2　　イ　4　　ウ　5　　エ　10

問 23　CSMA 方式の LAN 制御に関する記述として，適切なものはどれか。

ア　キャリア信号を検出しデータの送信を制御する。

イ　送信権をもつメッセージ（トークン）を得た端末がデータを送信する。

ウ　データ送信中に衝突が起こった場合は，直ちに再送を行う。

エ　伝送路が使用中でもデータの送信はできる。

問 24　FDDI における送信権制御に関する記述として，適切なものはどれか。

ア　各ノードは，他ノードが伝送媒体に送信した信号の有無を調べ，なければ送信を行う。これによって，送信競合の頻度を低減する。

イ　トークンと呼ばれる特殊な電文をノードからノードへ巡回させ，送信要求のあるノードは，トークンを受信したときに送信権を得る。

ウ　マスタコントローラは，各ノードから送信メッセージを受け取り，あて先に中継することによって，送信競合を防ぐ。

エ　マスタコントローラは，各ノードに送信要求の有無を問い合わせ，送信要求のあるノードに送信権を与える。

問 25　スパニングツリー機能を説明したものはどれか。

ア　MAC アドレスを見て，フレームを廃棄するか中継するかを決める。

イ　一定時間通信が行われていない MAC アドレスを，MAC アドレステーブルから消去する。

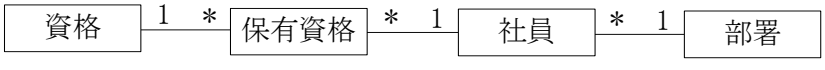
ウ　経路が複数存在する場合，アプリケーションやアドレスごとに経路を振り分けて，負荷を分散する。

エ　複数のブリッジ間で情報を交換し合い，ループ発生の検出や障害発生時の迂回ルート決定を行う。

問 26　次のような社員一覧表を分析し，図のようなデータモデルを作成した。“社員”エンティティを関係スキーマで表したものとして，適切なものはどれか。ここで，＊　1 は関連の多重度を表す。

社員一覧表

社員名	年齢	勤続年数	住所	保有資格	所属
鈴木　一郎	40	18	千葉県…	テクニカルエンジニア（データベース）	総務部
佐藤　浩子	30	8	東京都…	ソフトウェア開発技術者	経理部
⋮	⋮	⋮	⋮	⋮	⋮



データモデル

ア　社員（社員番号，氏名，生年月日，入社年月日，住所）

イ　社員（社員番号，氏名，生年月日，入社年月日，住所，年齢，勤続年数）

ウ　社員（社員番号，氏名，生年月日，入社年月日，住所，部署コード）

エ　社員（社員番号，氏名，生年月日，入社年月日，住所，保有資格件数）

問 27　ビューの SELECT 権限に関する記述のうち，適切なものはどれか。

ア　ビューに対して問合せするには，ビューに対する SELECT 権限だけではなく，元の表に対する SELECT 権限も必要である。

イ　ビューに対して問合せするには，ビューに対する SELECT 権限又は元の表に対する SELECT 権限のいずれかがあればよい。

ウ　ビューに対する SELECT 権限にかかわらず，元の表に対する SELECT 権限があれば，そのビューに対して問合せすることができる。

エ　元の表に対する SELECT 権限にかかわらず，ビューに対する SELECT 権限があれば，そのビューに対して問合せすることができる。

問 28　データベースの障害回復処理に関する記述のうち，適切なものはどれか。

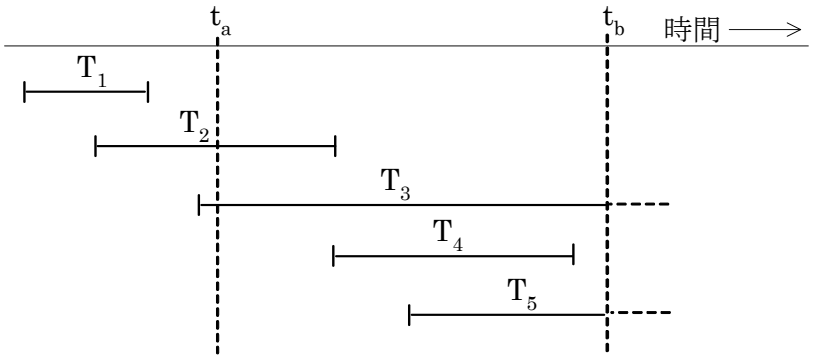
ア　異なるトランザクション処理プログラムが，同一データベースを同時更新することによって生じる論理的な矛盾を防ぐために，データのブロック化が必要となることがある。

イ　データベースの物理的障害に対して，バックアップファイルをリストアした後，ログファイルの更新前情報を使用してデータの回復処理を行う。

ウ　トランザクション処理プログラムがデータベースの更新中に異常終了した場合には，ログファイルの更新後情報を使用してデータの回復処理を行う。

エ　トランザクション処理プログラムでデータベースの更新頻度が多い場合には，チェックポイントを設定してデータの回復に備えることがある。

問 29　図に示すトランザクション T_1 から T_5 を処理するデータベースシステムにおいて，時刻 t_b にシステム障害が発生した。それ以前の最新のチェックポイントが時刻 t_a であったとして，ログ情報を基にロールフォワードによって復旧するトランザクションはどれか。ここで，ログ情報は収集されているものとする。また，図中の ├──┤ は，トランザクションの開始から終了までの時間を表す。



ア　T_1　　イ　T_1 と T_2　　ウ　T_2 と T_4　　エ　T_3 と T_5

問 30　分散データベースシステムのデータディクショナリ／ディレクトリの配置方式に関する記述のうち，適切なものはどれか。

ア　集中管理方式では，データディクショナリ／ディレクトリを保有するサイトに負荷が集中することはない。

イ　集中管理方式では，データディクショナリ／ディレクトリを保有するサイトの障害が，分散データベースの重大な障害になる。

ウ　分散管理方式で，各サイトにデータディクショナリ／ディレクトリを重複保有しない形態では，表の構造の変化が発生した場合，すべてのサイトで内容を変更する必要がある。

エ　分散管理方式で，各サイトにデータディクショナリ／ディレクトリを重複保有する形態では，問合せに対して，ほかのサイトの内容を調べることがある。

問 31　分散データベースシステムにおける“分割に対する透過性”を説明したものはどれか。

ア　データの格納サイトが変更されても，ユーザのアプリケーションや操作法に影響がないこと

イ　同一のデータが複数のサイトに格納されていても，ユーザはそれを意識せずに利用できること

ウ　一つの表が複数のサイトに分割されて格納されていても，ユーザはそれを意識せずに利用できること

エ　ユーザがデータベースの位置を意識せずに利用できること

問 32　2 相コミットで分散トランザクションの原子性を保証する場合，ネットワーク障害の発生によって参加者のトランザクションが，コミットすべきかロールバックすべきかを判断できなくなることがある。このような状況を発生させるネットワーク障害に関する説明として，適切なものはどれか。

ア　調停者のトランザクションが，コミット又はロールバック可否の問合せを参加者に送る直前に障害になった。

イ　調停者のトランザクションが，コミット又はロールバックの決定を参加者に送る直前に障害になった。

ウ　調停者のトランザクションに，コミット又はロールバック可否の応答を参加者が返す直前に障害になった。

エ　調停者のトランザクションに，コミット又はロールバックの完了を参加者が返す直前に障害になった。

問 33　DBMS に実装すべき原子性（atomicity）を説明したものはどれか。

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 34　トランザクション管理の直列化可能スケジュールを説明したものはどれか。

ア　デッドロックの発生を最小限に抑えるために，可能な限りトランザクションを直列に実行するスケジュール

イ　トランザクションの前後関係を考慮しながら，処理時間が最短になるようにトランザクションを同時実行するスケジュール

ウ　トランザクションを順番に実行した場合と同じ結果をもつように，同時実行するスケジュール

エ　読取り専用トランザクションは同時実行するが，更新を行うトランザクションは直列に実行するスケジュール

問 35　DBMS において用いられるデータ格納形式のうち，レコード数に応じて索引を階層化し，オーバフローエリアをもたず，根から葉までの深さが一定な方式はどれか。

ア　B^+木　　イ　索引付ファイル

ウ　ハッシュファイル　　エ　ヒープファイル

問 36　公開鍵暗号方式に関する記述として，適切なものはどれか。

ア　AES などの対称鍵暗号方式があり，鍵の配送は必要ない。

イ　RSA や楕円曲線暗号などがあり，復号時には暗号化鍵は使用しない。

ウ　暗号化鍵と復号鍵が同一である。

エ　共通鍵の配送が必要である。

問 37　公開鍵暗号方式によって，n 人が相互に暗号を使って通信する場合，異なる鍵は全体で幾つ必要になるか。

ア　$n+1$　　イ　$2n$　　ウ　$\frac{n(n-1)}{2}$　　エ　$\log_2 n$

問 38　XML ディジタル署名の特徴はどれか。

ア　XML 文書中の，指定したエレメントに対して署名することができる。

イ　エンベロープピング署名では一つの署名対象に必ず複数の署名を付ける。

ウ　署名形式として，CMS（Cryptographic Message Syntax）を用いる。

エ　署名対象と署名アルゴリズムを ASN. 1 によって記述する。

問 39　ディジタル証明書に関する記述のうち，適切なものはどれか。

ア　S/MIME や SET で利用するディジタル証明書の規格は，X. 400 で規定されている。

イ　ディジタル証明書は，SSL/TLS プロトコルで通信データの暗号化のための鍵交換や通信相手の認証に利用される。

ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局が電子署名したもので

ある。

エ　ルート認証局は，下位層の認証局の公開鍵にルート認証局の公開鍵で電子署名したディジタル証明書を発行する。

問 40　公開鍵暗号方式によるディジタル署名の手続とハッシュ値の使用方法のうち，適切なものはどれか。

ア　受信者は，送信者の公開鍵で署名を復号してハッシュ値を取り出し，元のメッセージを変換して求めたハッシュ値と比較する。

イ　送信者はハッシュ値を自分の公開鍵で暗号化して，元のメッセージとともに受信者に送る。

ウ　ディジタル署名を付ける元となったメッセージは，署名を変換したハッシュ値から復元できる。

エ　元のメッセージ全体に対して公開鍵で暗号化を行い，ハッシュ値を用いて復号する。

問 41　SQL インジェクション攻撃を防ぐ方法はどれか。

ア　入力値から，上位ディレクトリを指定する文字（../）を取り除く。

イ　入力値から，データベースへの問合せや操作において特別な意味をもつ文字を取り除く。

ウ　入力値に HTML タグが含まれていたら，解釈，実行できないほかの文字列に置き換える。

エ　入力値の全体の長さが制限を超えていないかどうかチェックする。

問 42　Web ビーコンを説明したものはどれか。

ア　Web サイトからダウンロードされ，PC 上で画像ファイルを消去するウイルス

イ　Web サイトで用いるアプリケーションプログラムに潜在する誤り

ウ　悪意のあるスクリプトによって PC と Web サーバ自体の両方に被害を及ぼす不正な手口

エ　利用者のアクセス動向などの情報を収集するために Web ページなどに埋め込まれた画像

問 43　VBScript（Visual Basic Script）で作られたコンピュータウイルスの特徴はどれか。

ア　HTML 形式の電子メール本文などに埋め込まれたスクリプトによって動作する。

イ　感染対象が実行形式ファイルであるか文書ファイルであるかにかかわらず，すべての OS で動

作する。

ウ　実行形式ファイルではなくワープロの文書ファイルなどに感染し，関連するアプリケーションソフトを利用して動作する。

エ　ブートセクタに感染して，通常のプロセス起動前にウイルスが呼び出されて動作する。

問 44　ブルートフォース攻撃に該当するものはどれか。

ア　コンピュータへのキー入力をすべて記録して外部に送信する。

イ　盗聴者が正当な利用者のログインシーケンスをそのまま記録してサーバに送信する。

ウ　認証が終了し，セッションを開始しているユーザとホストの間の通信で，クッキーなどのセッション情報を取る。

エ　文字を組み合わせてあらゆるパスワードでログインを何度も試みる。

問 45　表に示すテーブル X, Y へのアクセス要件に関して，JIS Q 27001:2006 (ISO/IEC 27001:2005) が示す“完全性”の観点からセキュリティを脅かすおそれのあるテーブルへのアクセス権付与はどれか。

テーブル	アクセス要件
X（注文テーブル）	①　調達課のユーザ A が注文データを入力したり内容を確認したりするためにアクセスする。 ②　管理課のユーザ B はアクセスしない。
Y（仕入先マスタテーブル）	①　調達課のユーザ A が仕入先データを照会する目的だけでアクセスする。 ②　管理課のユーザ B が仕入先データのマスタメンテナンス作業を行うためにアクセスする。

ア　`GRANT INSERT ON Y TO A`　　イ　`GRANT INSERT ON Y TO B`

ウ　`GRANT SELECT ON X TO A`　　エ　`GRANT SELECT ON X TO B`

問 46　パスワードに使用できる文字の種類の数を M，パスワードの文字数を n とするとき，設定できるパスワードの総数を求める数式はどれか。

ア　M^n　　イ　$\dfrac{M!}{(M-n)!}$

ウ　$\frac{M!}{n!(M-n)!}$　　エ　$\frac{(M+n-1)!}{n!(M-1)!}$

問 47　ソーシャルエンジニアリングに該当する行為はどれか。

ア　OS のセキュリティホールを突いた攻撃を行う。

イ　コンピュータウイルスを作る。

ウ　パスワードを辞書攻撃で破ってコンピュータに侵入する。

エ　本人を装って電話をかけ，パスワードを聞き出す。

問 48　DMZ 上の公開 Web サーバで入力データを受け付け，内部ネットワークの DB サーバにそのデータを蓄積するシステムがある。DB サーバへの不正侵入を防ぐファイアウォールの有効な設定はどれか。

ア　DB サーバの受信ポートを固定にし，Web サーバから DB サーバの受信ポートへ発信された通信だけをファイアウォールで通す。

イ　Web サーバの発信ポートは任意のポート番号を使用し，ファイアウォールでは，いったん終了した通信と同じ発信ポートを使った通信を拒否する。

ウ　Web サーバの発信ポートを固定し，その発信ポートの通信だけをファイアウォールで通す。

エ　ファイアウォールで，DB サーバあての受信パケットだけ通す。

問 49　HTTPS を用いて実現できるものはどれか。

ア　Web サーバ上のファイルの改ざん検知

イ　クライアント上のウイルス検査

ウ　クライアントに対する侵入検知

エ　電子証明書によるサーバ認証

問 50　セキュリティプロトコル SSL/TLS の機能はどれか。

ア　FTP などの様々なアプリケーションに利用されて，アプリケーション層と TCP との間で暗号

化する。

イ　MIME をベースとして，電子署名とメッセージの暗号化によって電子メールのセキュリティを強化する。

ウ　PPTP と L2F が統合された仕様で，PPP をトンネリングする。

エ　特定のアプリケーションの通信だけではなく，あらゆる IP パケットを IP 層で暗号化する。

問 51　情報システムのリスク分析における作業①～⑤の，適切な順序はどれか。

① 損失の分類と影響度の評価
② 対策の検討・評価と優先順位の決定
③ 事故態様の関連分析と損失額予想
④ 脆弱性の発見と識別
⑤ 分析対象の理解と分析計画

ア　④ → ⑤ → ② → ③ → ①　　イ　④ → ⑤ → ③ → ② → ①
ウ　⑤ → ④ → ② → ③ → ①　　ア　⑤ → ④ → ③ → ① → ②

問 52　“JIS Q 9001:2000（ISO 9001:2000）品質マネジメントシステム－要求事項”に規定されている経営者の責任はどれか。

ア　経営者は，品質マネジメントシステムの構築，実施及び改善に対するコミットメントの証拠を示さなければならない。

イ　組織内の部門，階層ごとの品質目標は，経営者が設定しなければならない。

ウ　品質管理の責任は経営者にあるので，権限を委譲することなく，必要なプロセスの確立，実施及び維持を確実にしなければならない。

エ　不具合又は不満足な状況に陥った場合，それが是正されるまで，経営者は後工程への進行を止めなければならない。

問 53　JIS X 5070（ISO/IEC 15408）の評価保証レベル EAL4 に相当するものはどれか。

ア　ガイダンス文書の検査や機能仕様書とインタフェース仕様書によって，セキュリティ機能を確認するレベル

イ　開発者によって実施されたテスト範囲の検査や開発環境で改ざんが起きないことを確認する

レベル

ウ　概要設計書の検査や開発者が行ったテスト結果及び脆弱性評価を対象に確認するレベル

エ　詳細設計書と一部のソースコードや製造図面など，実装を確認するレベル

問 54　“JIS Q 27001:2006（ISO/IEC 27001:2005）情報セキュリティマネジメントシステム－要求事項”に規定されているものはどれか。

ア　ISMS が適切に運用されているかどうかを評価するために，定期的に外部監査を受けなければならない。

イ　経営者の責任が重要であり，コミットメント，経営資源の提供，マネジメントレビューなどに関与しなければならない。

ウ　附属書の管理策は，すべて適用しなければならない。

エ　リスクアセスメントで明らかになったすべてのリスクに対して，リスク管理策を適用しなければならない。

問 55　世界各国の文字体系に対応できるように ISO/IEC で規格化された文字コード体系 ISO/IEC 10646 では，文字を 16 ビット又は 32 ビットで表す。このコード体系で 16 ビット表現を用いるサブセットはどれか。

ア　Extended Unix Code　　イ　JIS コード

ウ　UCS-2（Unicode）　　エ　シフト JIS コード