平成１８年度　秋期　情報セキュリティアドミニストレータ　午前問題

問１　ページング方式の仮想記憶におけるページサイズに関する記述のうち，適切なものはどれか。

ア　仮想アドレス空間ごとに異なるが，一つの仮想アドレス空間内では同一である。

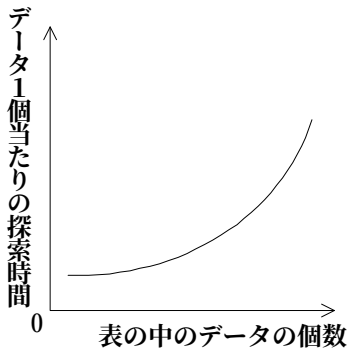
イ　コンピュータのアーキテクチャによって取り得るサイズが定められている。

ウ　その時点で最適なサイズに，動的に変更される。

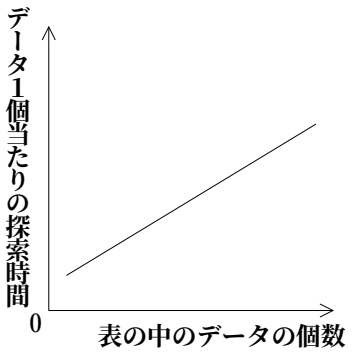
エ　プログラムが 1 ページに収まるようにするために，プログラムごとに異なる。

問２　ハッシュ表の理論的な探索時間を示すグラフはどれか。ここで，シノニムは発生しないものとする。

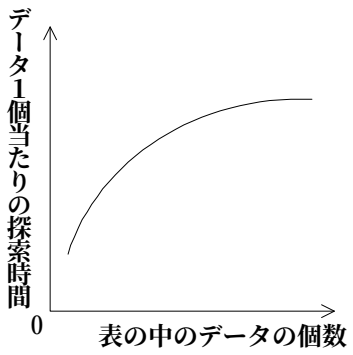
ア



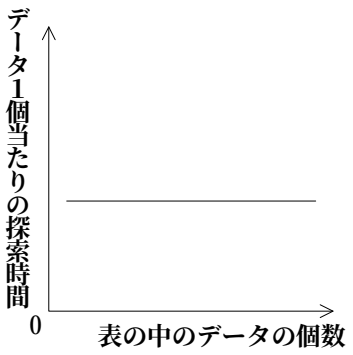
イ



ウ



エ



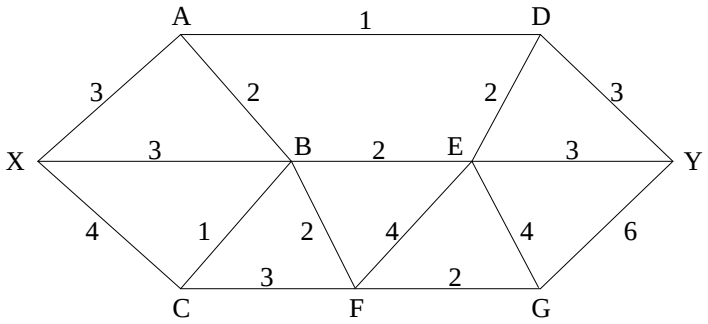
問３　マルチプロセッサによる並列処理で得られる高速化率（単一プロセッサのときと比べた倍率）E を，次の式によって評価する。r = 0.9 のアプリケーションの高速化率が r = 0.3 のものの 3 倍となるのは，プロセッサが何台のときか。

$$E = \frac{1}{1 - r + r/n}$$

ここで，
n：プロセッサの台数（1 ≦ n）
r：対象とする処理のうち，並列化が可能な部分の割合（0 ≦ r ≦ 1）
とし，並列化に伴うオーバヘッドは考慮しないものとする。

ア　3　　イ　4　　ウ　5　　エ　6

問４　次のネットワーク図の数値は，二つの地点の間に同時に設定できる論理回線の多重度を示している。このうち，多重度を 1 だけ大きくすることによって，XY 間に設定できる最大論理回線数を増やせる区間はどれか。



ア　AB　　イ　BF　　ウ　ED　　エ　FE

問５　データマイニングツールに関する記述として，最も適切なものはどれか。

ア　企業内で発生する情報を主題ごとに時系列で蓄積することによって，既存の情報システムだけでは得られない情報を提供する。

イ　集計データを迅速かつ容易に表示するなど，利用者に対して様々な情報分析機能を提供する。

ウ　大量に蓄積されたデータに対して統計処理などを行い，法則性の発見を支援する。

エ　利用者が情報を利用するための目的別データベースであり，あらかじめ集計処理などを施して

おくことによって検索時間を短縮する。

問６　データベースのメタデータについて説明したものはどれか。

ア　集合をメンバ（インスタンス）として扱う“べき集合”

イ　属性がもつことのできる値の範囲

ウ　データ管理者が管理し，DBMS には登録しない情報

エ　データの定義情報を記述したデータ

問７　CMMI の目的はどれか。

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の向上を図る。

イ　ソフトウェアライフサイクルを，主，支援及び組織に関する三つのライフサイクルプロセスに分けてアクティビティを定め，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。

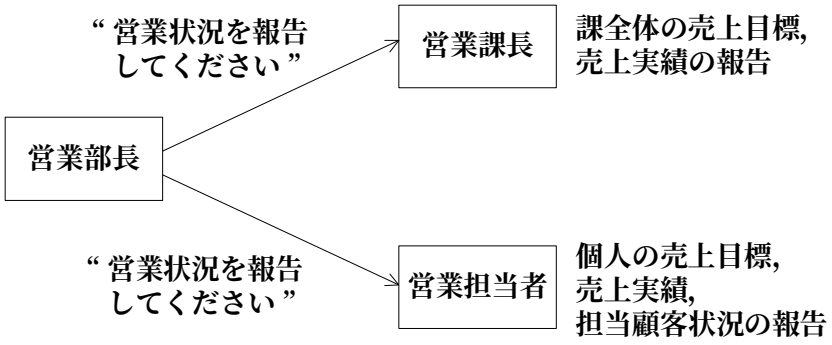
エ　特定の購入者と製作者の間で授受されるソフトウェア製品の品質保証を行い，顧客満足度の向上を図る。

問８　UML で用いる図のうち，オブジェクト間で送受信するメッセージによる相互作用が表せるものはどれか。

ア　コンポーネント図　　イ　シーケンス図

ウ　ステートチャート図　　エ　ユースケース図

問９　図において，“営業状況を報告してください”という同じ指示（メッセージ）に対して，営業課長と営業担当者は異なる報告（サービス）を行っている。オブジェクト指向で，このような特性を表す用語はどれか。



・営業部長が，営業課長と営業担当者へ“営業状況を報告してください”という指示を送る。
・営業課長が，課全体の売上目標，売上実績の報告を応答する。
・営業担当者が，本人の売上目標，売上実績，担当顧客状況の報告を応答する。

ア　カプセル化　　イ　継承　　ウ　抽象化　　エ　ポリモーフィズム

問 10　フールプルーフに該当するものはどれか。

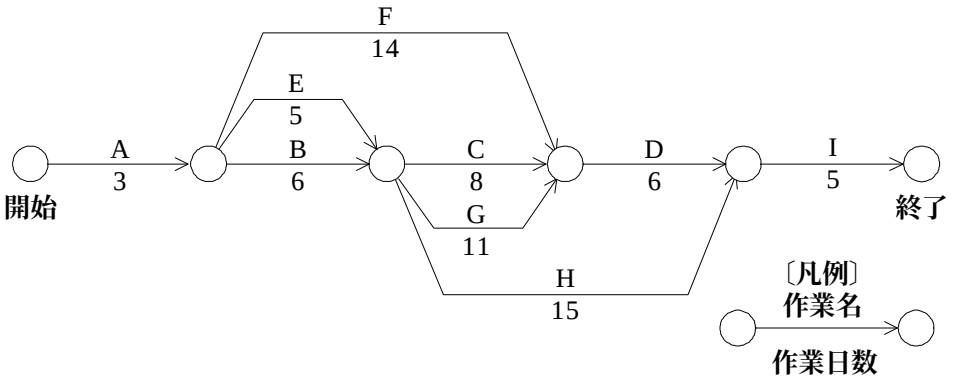
ア　更新の対象となるものをコピーして保存する。

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 11　図は，あるプロジェクトの作業（A～I）とその作業日数を表している。このプロジェクトが終了するまでに必要な最短日数は何日か。



ア　27　　イ　28　　ウ　29　　エ　31

問 12　**レプリケーションが有効な対策となるものはどれか。**

ア　**悪意による改ざんをなくす。**

イ　**ウイルスによるデータ破壊をなくす。**

ウ　**災害発生時に短時間で復旧する。**

エ　**操作ミスによるデータの削除を防ぐ。**

問 13　SLA **の説明はどれか。**

ア　**開発から保守までのソフトウェアライフサイクルプロセス**

イ　**サービスの品質に関する利用者と提供者間の合意**

ウ　**システムの運用手法を体系化したフレームワーク**

エ　**製品ベンダの品質マネジメントシステムに関する国際規格**

問 14　TCP/IP **ネットワークで使用される** ARP **の説明として，適切なものはどれか。**

ア　IP **アドレスから** MAC **アドレスを得るためのプロトコル**

イ　IP **アドレスからホスト名（ドメイン名）を得るためのプロトコル**

ウ　MAC **アドレスから** IP **アドレスを得るためのプロトコル**

エ　**ホスト名（ドメイン名）から** IP **アドレスを得るためのプロトコル**

問 15　TCP/IP **のクラス** B **の** IP **アドレスをもつ一つのネットワークに，割り当てることができるホストアドレス数はどれか。**

ア　1,022　　**イ**　4,094　　**ウ**　32,766　　**エ**　65,534

問 16　**サブネットマスクが** 255.255.252.0 **のとき，**IP **アドレス** 172.30.123.45 **のホストが属するサブネットワークのアドレスはどれか。**

ア　172.30.3.0　　**イ**　172.30.120.0　　**ウ**　172.30.123.0　　**エ**　172.30.252.0

問 17　TCP/IP 環境において，複数のコンピュータで時刻同期をとるためのプロトコルはどれか。

ア　LCP　　イ　NCP　　ウ　NTP　　エ　RTP

問 18　WAN を介して二つのノードをダイヤルアップ接続するときに使用されるプロトコルで，リンク制御やエラー処理機能をもつものはどれか。

ア　FTP　　イ　PPP　　ウ　SLIP　　エ　UDP

問 19　無線 LAN（IEEE 802.11b）で使用されるデータ暗号化方式はどれか。

ア　SSID　　イ　SSL　　ウ　WAP　　エ　WEP

問 20　動画符号化の国際規格である MPEG-1 に関する記述として，最も適切なものはどれか。

ア　CD-ROM などを蓄積メディアとして想定した動画像圧縮符号化の規格である。

イ　DVD-Video やディジタル衛星放送で使用される高品質の動画像圧縮符号化の規格である。

ウ　携帯端末などに用いられる低速回線用の動画像圧縮符号化の規格である。

エ　複数の JPEG 画像の連続表示で動画を実現するための規格である。

問 21　米国 NIST が採用した AES（Advanced Encryption Standard）における鍵長の条件はどれか。

ア　128，192，256 ビットから選択する。

イ　256 ビット未満で任意に指定する。

ウ　暗号化処理単位のブロック長より 32 ビット大きくする。

エ　暗号化処理単位のブロック長より 32 ビット小さくする。

問 22　100 人の送受信者が共通鍵暗号方式で，それぞれ秘密に通信を行うときに必要な共通鍵の総数は幾つか。

ア　200　　イ　4,950　　ウ　9,900　　エ　10,000

問 23　公開鍵暗号方式の用法によって，送信者が間違いなく本人であることを受信者が確認できる鍵の組合せはどれか。

ア　送信者は自分の公開鍵で暗号化し，受信者は自分の秘密鍵で復号する。

イ　送信者は自分の秘密鍵で暗号化し，受信者は送信者の公開鍵で復号する。

ウ　送信者は受信者の公開鍵で暗号化し，受信者は自分の秘密鍵で復号する。

エ　送信者は受信者の秘密鍵で暗号化し，受信者は自分の公開鍵で復号する。

問 24　社内のセキュリティポリシで，利用者の事故に備えて秘密鍵を復元できること，及びセキュリティ管理者の不正防止のための仕組みを確立することが決められている。電子メールで公開鍵暗号方式を使用し，鍵の生成はセキュリティ部門が一括して行っている場合，秘密鍵の適切な保管方法はどれか。

ア　1 人のセキュリティ管理者が，秘密鍵を暗号化して保管する。

イ　暗号化された秘密鍵の一つ一つを分割し，複数のセキュリティ管理者が分担して保管する。

ウ　セキュリティ部門には，秘密鍵を一切残さず，利用者本人だけが保管する。

エ　秘密鍵の一覧表を作成して，セキュリティ部門内に限り参照できるように保管する。

問 25　シングルサインオンの説明のうち，適切なものはどれか。

ア　クッキーを使ったシングルサインオンでは，サーバごとの認証情報を含んだクッキーをクライアントで生成し，各サーバ上で保存・管理する。

イ　クッキーを使ったシングルサインオンでは，認証対象の各サーバをそれぞれ異なるインターネットドメインにする必要がある。

ウ　リバースプロキシを使ったシングルサインオンでは，認証対象の各 Web サーバをそれぞれ異なるインターネットドメインにする必要がある。

エ　リバースプロキシを使ったシングルサインオンでは，ユーザ認証においてパスワードの代わりにディジタル証明書を用いることができる。

問 26　コンピュータウイルスの検出，機能の解明，又は種類の特定をする手法について，適切な記述はどれか。

ア　暗号化された文書中のマクロウイルスを検出するにはパターンマッチング方式が有効である。

イ　逆アセンブルは，バイナリタイプの新種ウイルスの機能を解明するのに有効な手法である。

ウ　不正な動作を識別してウイルスを検知する方式は，ウイルス名を特定するのに最も有効である。

エ　ワームは既存のファイルに感染するタイプのウイルスであり，その感染の有無の検出にはファイルの大きさの変化を調べるのが有効である。

問 27　メッセージの改ざんを検出するためのメッセージ認証符号 MAC について説明したものはどれか。

ア　送信者と受信者の共通鍵を元に，メッセージにハッシュ関数を適用して生成したもの

イ　メッセージにハッシュ関数を適用して得たデータを送信者の秘密鍵で暗号化したもの

ウ　メッセージを一定のビット数のブロックに分割し，各ブロックのデータを数値として加算した総和の値から，一定の計算をして求めたもの

エ　メッセージを構成する各バイトに含まれる“1”のビットの個数が奇数になるように，最下位ビットの値を調整したもの

問 28　クロスサイトスクリプティングによる攻撃へのセキュリティ対策はどれか。

ア　OS のセキュリティパッチを適用することによって，Web サーバへの侵入を防止する。

イ　Web アプリケーションで，クライアントに入力データを再表示する場合，情報内のスクリプトを無効にする処理を行う。

ウ　Web サーバに SNMP プログラムを常駐稼働させることによって，攻撃を検知する。

エ　許容範囲を超えた大きさのデータの書込みを禁止し，Web サーバへの侵入を防止する。

問 29　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，ディ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 30　セキュリティ上，脆弱性のあるホストやシステムをあえて公開し，受けた攻撃の内容を観察するためのものはどれか。

ア　IDS　　イ　インシデントレスポンス

ウ　スパイウェア　　エ　ハニーポット

問 31　S/MIME で実現できるものはどれか。

ア　SSL を利用して電子メールを暗号化する。

イ　共通鍵で電子メールの送信者を認証する。

ウ　受信側が S/MIME に対応していなくても，暗証キーを入力して復号する。

エ　電子メールの改ざんを検出する。

問 32　TLS について説明したものはどれか。

ア　相手が秘密鍵をもっているかどうかを検証するために，乱数を送付し，署名してもらう認証

イ　トランスポート層において，アプリケーションとは独立に暗号化及びディジタル署名を施すことを可能にした規約

ウ　複数の LAN やコンピュータシステムを，インターネットや共用回線を用いて仮想的に同一ネットワークとして安全に接続する技術

エ　ルータ間の通信の秘匿性，相手認証，パケットごとの改ざん防止を提供するためのプロトコル

問 33　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，暗号化された HTML 文書はブラウザでキャッシュの有無が設定できずディスク内に必ず保存される。

問 34　ISMS では，情報セキュリティは三つの事項を維持するものとして特徴付けられている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。

ア　安全性　　イ　可用性　　ウ　効率性　　エ　保守性

問 35　企業内情報ネットワークやサーバへの外部からのアクセスにおいて，通常の経路以外で，侵入者が不正な行為に利用するために設置するものはどれか。

ア　VoIP ゲートウェイ　　イ　ストリクトルーティング

ウ　バックドア　　エ　フォレンジクス

問 36　ISMS におけるリスク分析の方法の一つであるベースラインアプローチはどれか。

ア　公表されている基準などに基づいて一定のセキュリティレベルを設定し，実施している管理策とのギャップ分析を行った上で，リスクを評価する。

イ　情報資産を洗い出し，それぞれの情報資産に対して資産価値，脅威，脆弱性及びセキュリティ要件を識別し，リスクを評価する。

ウ　複数のリスク分析方法の長所を生かして組み合わせ，作業効率や分析精度の向上を図る。

エ　リスク分析を行う組織や担当者の判断によって，リスクを評価する。

問 37　TR X 0036-1:2001（IT セキュリティマネジメントのガイドライン－第 1 部：IT セキュリティの概念及びモデル）では，情報資産に対する脅威の例を表のように分類している。表の b に入るものはどれか。

脅威の分類		脅威の例
a	b	盗聴，情報の改ざん
	c	誤り及び手落ち，物理的な事故
d		地震，落雷

ア　意図的　　イ　環境　　ウ　偶発的　　エ　人間

問 38　システム開発と取引のための共通フレーム（SLCP-JCF98）の目的はどれか。

ア　ISO/IEC の SLCP の検討内容を基にして，対象範囲に企画プロセスとシステム監査プロセスを加え，ソフトウェア取引に関する提案責任と管理責任を明確にすること

イ　システム開発作業全般にわたって“共通の物差し”や“共通語”を使うことによって，作業範囲・作業内容を明確にし，購入者と供給者の取引を明確にすること

ウ　ソフトウェアを適切に購入・使用するためのガイドラインを示すことによって，ソフトウェアの違法複製行為や違法複製品の使用を防止し，ソフトウェアの適正な取引及び管理を促進すること

エ　特定の業種やシステム形態，開発方法論などに極力依存しないよう配慮し，社内の部門間での取引を除く受発注契約をスムーズに遂行すること

問 39　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　暗号アルゴリズムの標準

イ　情報技術に関するセキュリティの評価基準

ウ　情報セキュリティ管理の実施基準

エ　セキュリティ管理のプロトコルの標準

問 40　SAML（Security Assertion Markup Language）について説明したものはどれか。

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　ディジタル署名に使われる鍵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

問 41　文字コードに関する記述のうち，適切なものはどれか。

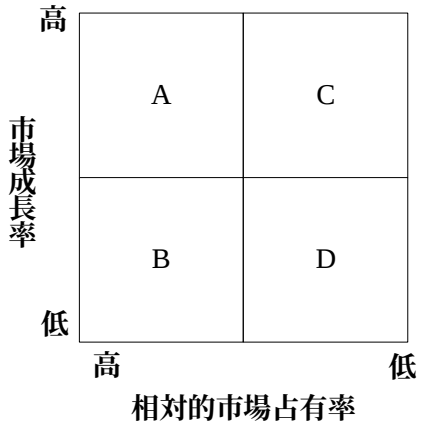
ア　EBCDIC は，汎用コンピュータに利用されている 2 バイトコードである。

イ　EUC は，サーバの多言語対応をサポートするコードであり，日本語環境では 4 バイトからなるコード表現を採用している。

ウ　Unicode は ISO 規格化された文字コードであり，2 バイト（ucs-2），4 バイト（ucs-4）で定義されている。

エ　シフト JIS コードは，1 バイトの文字コードと 2 バイトの文字コードを制御符号を用いて混在させている。

問 42　PPM の各領域をプロダクトライフサイクル上の各時期に当てはめたとき，領域 A に分類される製品はどの時期に対応しているか。



ア　衰退期　　イ　成熟期　　ウ　成長期　　エ　導入期

問 43　大量生産・大量販売のメリットを生かしつつ，きめ細かな仕様・機能の取込みなどによって，顧客一人一人の好みに応じられる製品やサービスを提供しようとするものはどれか。

ア　ターゲットマーケティング　　イ　ベストプラクティス

ウ　ベネフィットセグメンテーション　　エ　マスカスタマイゼーション

問 44　問題解決能力の育成方法で，日常起こるマネジメント上の問題を多数提示して，一定時間内に判断し処理させる手法はどれか。

ア　KJ 法　　イ　インバスケット

ウ　ケーススタディ　　エ　ロールプレイ

問 45　エンタープライズアーキテクチャを説明したものはどれか。

ア　今まで開発してきた業務システムをビジネス価値とソリューション品質の 2 軸で分析し，業務システムごとの改善の方向を決定する。

イ　既存の業務と情報システムの全体像及び将来の目標を明示することによって，IT ガバナンスを強化し，経営の視点から IT 投資効果を高める。

ウ　財務，顧客，業務プロセス，学習・成長の四つの視点から評価指標を設定し，IT 投資による組織全体への効果を的確に管理する。

エ　情報システムの開発・保守とその組織運営の現状を調査し，ソフトウェアプロセスの成熟度を評価して，プロセス改善の方向を決定する。

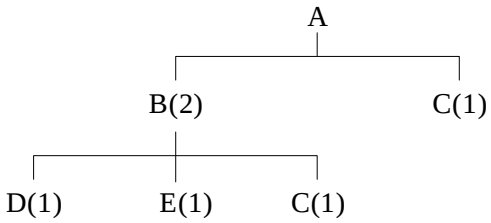
問 46　ある営業部員の 1 日の業務活動を分析した結果は，表のとおりである。営業支援システムの導入によって訪問準備時間が 1 件当たり 0.1 時間短縮できる。総業務時間と 1 件当たりの顧客訪問時間を変えずに，1 日の顧客訪問件数を 6 件にするには，“ その他業務時間 ”を何時間削減する必要があるか。

1日の業務活動の時間分析表

総業務時間					1日の顧客訪問件数
	顧客訪問時間	社内業務時間			
			訪問準備時間	その他業務時間	
8.0	5.0	3.0	1.5	1.5	5件

ア　0.3　　イ　0.5　　ウ　0.7　　エ　1.0

問 47　図は，製品 A の構成部品を示している。この製品 A を 10 個生産する場合，部品 C の手配数量は何個になるか。ここで，（　）内の数字は上位部品 1 個当たりの所要数量であり，部品 C の在庫は 5 個とする。



ア　15　　イ　20　　ウ　25　　エ　30

問 48　インターネットを利用した企業間取引において，取引データをそのまま起票したり，社内文書に変換したりすることが容易にできるマーク付け言語はどれか。

ア　HTML　　イ　SGML　　ウ　UML　　エ　XML

問 49　インタラクティブ送信における著作権に関する記述のうち，適切なものはどれか。

ア　サーバに蓄積された情報を，著作権者の許諾なしに送信可能な状態にするだけでは権利侵害とならない。

イ　著作権者の許諾なしに公衆に情報を送信する行為は，サーバに情報を蓄積するか否かにかかわらず権利侵害となる。

ウ　著作権者の許諾なしに送信された情報を，第三者が正常に受信できた場合に限り，権利侵害となる。

エ　著作権者の送信権は有線の場合に限って発生するものであり，無線の場合は権利侵害の対象とならない。

問 50　著作権法に関する記述のうち，適切なものはどれか。

ア　データベースを保護の対象としていない。

イ　プログラム言語や規約を保護の対象としていない。

ウ　プログラムのアイディアを保護している。

エ　プログラムの複製行為をすべて禁止している。

問 51　プロジェクトマネージャの P 氏は，A 社から受託予定のソフトウェア開発を行うために，X 社から一時的な要員派遣を受けることを検討している。労働者派遣法に照らして適切なものはどれか。

ア　厳しいスケジュールが見込まれることから，期間内での担当業務の完遂を条件とし，未達の場合に備えてペナルティ条項を記した契約案を X 社に提示した。

イ　前回のプロジェクトの成功に大きく貢献した X 社の Y 氏の参加を指名した。

ウ　派遣される要員のスキルを適切に判断しようと考え，事前に X 社の派遣候補者を面接した。

エ　派遣者への業務指示など，派遣に伴う各種業務を P 氏が直接行うことを X 社に伝えた。

問 52　メーカの A 社は，A 社が設計し B 社がコーディングしたソフトウェアを ROM に組み込み，その ROM を部品とした製品 X を製造し，販売会社である C 社に卸している。C 社は，この製品 X に“製造元 A 社”と表示し，一般消費者に販売した。ある消費者が購入した製品 X を使用したところ，ROM に組み込まれたソフトウェアの欠陥によってけがをした。原因はソフトウェアの設計ミスであった。製造物責任法（PL 法）上，製造物責任を問われる企業はどれか。

ア　A　　イ　A と B　　ウ　A と C　　エ　A と B と C

問 53　情報システムの監査証跡に関する記述のうち，適切なものはどれか。

ア　アクセスログやオペレーションログは，効率性のコントロールに関する監査証跡になる。

イ　監査証跡は，必要に応じて妥当な時間内で閲覧できることが要求されるので，紙に記録する。

ウ　処理過程をすべて記録しておくことは経済性を損なうおそれがあるので，必要十分な監査証跡を決定することが大切である。

エ　利用者ニーズの調査結果や費用対効果分析表は，信頼性のコントロールに関する監査証跡になる。

問 54　監査対象である開発プロジェクトは開発期間 12 か月，開発費用 3,000 万円であり，予想される期待効果は，稼働開始後 1 年間は 1,000 万円，2 年目からは月間 200 万円が見込まれる。また，システムの運用費用は毎月 100 万円である。

このプロジェクトの単純回収期間法による投資回収期間は，稼働開始を基点として何年何か月になるか。ただし，開発期間 12 か月で稼働開始できたものとする。

ア　2 年 8 か月　　イ　3 年 8 か月　　ウ　4 年 8 か月　　エ　回収不能

問 55　システム開発を外部委託した場合の品質管理の妥当性を確認するための監査項目はどれか。

ア　委託先が開発中の成果物に対するアクセス管理を厳格に行っていることを，委託元が確認しているか。

イ　委託元と委託先の間で，成果物の不具合に対する委託先の損害賠償責任に関する条項を盛り込んだ業務委託契約を締結しているか。

ウ　委託元は開発工程の決められた時点で成果物のレビューを行い，問題点が委託先によって解決されていることを確認しているか。

エ　開発スケジュールに対する作業実績について，委託元は委託先から週次で報告を受け，問題があったとき速やかに対応しているか。