問題

問 1

正解 □ 完璧 □ 直前CHECK □

特定のCAが発行したCRL（Certificate Revocation List）に関する記述のうち，適切なものはどれか．

ア　CRLには，失効された公開鍵証明書に対応する秘密鍵が登録される．
イ　CRLには，有効期限内の公開鍵証明書のうち破棄されている公開鍵証明書と破棄された日時の対応が提示される．
ウ　CRLは，鍵の漏えい，破棄申請の状況をリアルタイムに反映するプロトコルである．
エ　有効期限切れで無効になった公開鍵証明書は，所有者が新たな公開鍵証明書を取得するまでの間，CRLに登録される．

問 2

正解 □ 完璧 □ 直前CHECK □

IEEE 802.1Xで使われるEAP-TLSによって実現される認証はどれか．

ア　CHAPを用いたチャレンジレスポンスによる利用者認証
イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証
ウ　ディジタル証明書による認証サーバとクライアントの相互認証
エ　利用者IDとパスワードによる利用者認証

問 3

正解 □ 完璧 □ 直前CHECK □

SEO（Search Engine Optimization）ポイズニングの説明はどれか．

ア　Web検索サイトの順位付けアルゴリズムを悪用して，キーワードで検索した結果の上位に，悪意のあるサイトを意図的に表示させる．
イ　ウイルス検索エンジンのセキュリティ上の脆弱性を悪用して，システム権限で不正な処理を実行させる．
ウ　車などで移動しながら，無線LANのアクセスポイントを探し出して，ネットワークに不正侵入する．
エ　ネットワークを流れるパケットから，不正侵入のパターンに合致するものを検出して，管理者への通知や，検出した内容の記録を行う．

問1　イ

CRLは，有効期間中に失効した公開鍵証明書を記載したリストである．認証局から発行される．公開鍵証明書が失効しているかどうかの確認に使用する．公開鍵証明書の有効期間中に秘密鍵の紛失や漏えいが発生した場合には，該当する証明書の廃棄手続きが行われ，公開鍵証明書のシリアル番号がCRLに記載される．

ア：秘密鍵ではなく，破棄された証明書のリストが登録される．

ウ：破棄申請の状況を反映するのではなく，申請後の結果が公開される．

エ：CRLはCAが指定する期間公開される．所有者の公開鍵証明書取得までの間ではない．

問2　ウ

IEEE 802.1Xは，クライアントPCと，無線のアクセスポイントやスイッチングハブとの間で利用される，ディジタル証明書による認証プロトコルである．鍵交換により共有された鍵を用いて，クライアントPCと接続先との暗号化通信を行う．

IEEE 802.1Xでは，EAP-TLSやEAP-PEAPなどの認証方式が使用される．

EAP-TLS（Extensible Authentication Protocol - Transport Layer Security）：OSI第4層のトランスポート層に基づいて，ディジタル証明書による相互認証（サービス提供者の詐称をも防止する）を行う認証手順である．

問3　ア

SEO（Search Engine Optimization）は，インターネットのサーチエンジンで特定キーワードを検索した際に，対象となるWebページを検索結果の上位に表示させることである．**SEOポイズニング**は検索アルゴリズムを悪用し，悪意のあるサイトを意図的に上位に表示させることである．

意図的に表示されたサイトを利用して，詐欺行為やウイルスへの感染を誘導することが主な悪用方法となる．

イ：**不正アクセス**の説明である．

ウ：**ウォードライビング**の説明である．

エ：**NIDS**（Network Intrusion Detection System）の説明である．

問 4

正解 □ 完璧 □ 直前CHECK □

2011年に経済産業省が公表した“クラウドサービス利用のための情報セキュリティマネジメントガイドライン”が策定された目的について述べたものはどれか.

ア　JIS Q 27002の管理策を拡張し，クラウドサービス利用者が情報セキュリティ対策を円滑に行えるようにする.

イ　クラウドサービス提供事業者に対して情報セキュリティ監査を実施する方法を利用者に提示する.

ウ　クラウドサービスの利用がもたらすセキュリティリスクをサービス提供事業者の視点で提示する.

エ　セキュリティリスクの懸念の少ないクラウドサービス提供事業者を利用者が選択できるような格付け基準を提供する.

問 5

正解 □ 完璧 □ 直前CHECK □

スパムメールの対策として，宛先ポート番号25番の通信に対してISPが実施するOP25Bの説明はどれか.

ア　ISP管理外のネットワークからの通信のうち，スパムメールのシグネチャに該当するものを遮断する.

イ　動的IPアドレスを割り当てたネットワークからISP管理外のネットワークへの直接の通信を遮断する.

ウ　メール送信元のメールサーバについてDNSの逆引きができない場合，そのメールサーバからの通信を遮断する.

エ　メール不正中継の脆弱(ぜい)性をもつメールサーバからの通信を遮断する.

問4　ア

「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 序文 0.1 一般」には，「クラウド利用者の観点からJIS Q 27002（実践のための規範）の各管理策を考慮し，クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，このガイドを作成した」と記載されている．

イ，ウ，エ：このガイドラインは，組織がクラウドコンピューティングを全面的に利用する状態を想定して記載されているといえる．

問5　イ

OP25B（Outbound Port 25 Blocking）は，内部ネットワークから外部ネットワークへのポート25番の通信（SMTP）を遮断する手法である．

例えば，ISPがOP25Bを用いることで，会員がISPの外部ネットワークに存在するメールサーバを使用してスパムメールを送信しようとすることを防止することが可能となる．

問 6

正解 □ 完璧 □ 直前CHECK □

ファイアウォールにおけるダイナミックパケットフィルタリングの特徴はどれか.

ア　IPアドレスの交換が行われるので，ファイアウォール内部のネットワーク構成を外部から隠蔽できる.

イ　暗号化されたパケットのデータ部を復号して，許可された通信かどうかを判断できる.

ウ　戻りのパケットに関しては，過去に通過したリクエストパケットに対応したものだけを通過させることができる.

エ　パケットのデータ部をチェックして，アプリケーション層での不正なアクセスを防止できる.

問 7

正解 □ 完璧 □ 直前CHECK □

ポリモーフィック型ウイルスの説明として，適切なものはどれか.

ア　インターネットを介して，攻撃者がPCを遠隔操作する.

イ　感染するごとに鍵を変えてウイルスのコードを暗号化することによってウイルス自身を変化させて，同一のパターンで検知されないようにする.

ウ　複数のOSで利用できるプログラム言語でウイルスを作成することによって，複数のOS上でウイルスが動作する.

エ　ルートキットを利用してウイルスに感染していないように見せかけることによって，ウイルスを隠蔽する.

問 8

正解 □ 完璧 □ 直前CHECK □

FIPS 140-2を説明したものはどれか.

ア　暗号モジュールのセキュリティ要求事項

イ　情報セキュリティマネジメントシステムに関する認証基準

ウ　ディジタル証明書や証明書失効リストの標準仕様

エ　無線LANセキュリティ技術

問6　ウ

ダイナミックパケットフィルタリングは，ファイアウォールのパケット通過時のパケット開放の方式である．内部から外部への通信を実行した際に，外部からの戻りパケットもファイアウォールで開放する必要がある．ダイナミックパケットフィルタリングでは，戻りパケットを必要な状況に応じて動的に開放し，要求がない場合はポートを閉じておく方式である．

ア：IPアドレスの変換とは関係がない．

イ：パケットの暗号化は関係がない．

エ：パケットのデータ部分のチェックは行っていない．

問7　イ

ポリモーフィック型ウイルスは，感染するたびにウイルス自体を暗号化することにより，ウイルス対策ソフトから検知されないように振る舞うウイルスである．

暗号化されたコードは変化するが，ウイルスが発動するときの復号ロジックは変換しないという特徴がある．ウイルス対策ソフト側では，この特徴を利用してウイルス感染を検出する．

ア：**ハッキング**または**クラッキング**の説明である．

問8　ア

FIPS 140-2：暗号モジュールに関するセキュリティ要件仕様を規定する米国連邦標準規格．

イ：**BS 7799-2**や国内規格の**ISMS認証基準Ver.2.0**の後継として開発された国際規格および国内規格として，**ISO 27001**，**JIS Q 27001**がある．

ウ：インターネットのための**X.509 公開鍵基盤**（PKI）に対する標準がある．

エ：**IEEE 802.11**無線LANの国際規格の中では，セキュリティ技術として**SSID**（Service Set Identifier），**MACアドレスフィルタリング**，**WEP**（Wired Equivalent Privacy），**WPA2**（Wi-Fi Protected Access 2）などがある．

問題

問 9

正解 □ 完璧 □ 直前CHECK □

特定の情報資産の漏えいに関するリスク対応のうち，リスク回避に該当するものはどれか．

ア　外部の者が侵入できないように，入退室をより厳重に管理する．
イ　情報資産を外部のデータセンタに預託する．
ウ　情報の新たな収集を禁止し，収集済みの情報を消去する．
エ　情報の重要性と対策費用を勘案し，あえて対策をとらない．

問 10

正解 □ 完璧 □ 直前CHECK □

ICMP Flood攻撃に該当するものはどれか．

ア　pingコマンドを用いて同時に発信した大量の要求パケットによって，攻撃対象のサーバに至るまでの回路を過負荷にしてアクセスを妨害する．
イ　繰り返しHTTP GETコマンドを送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける．
ウ　コネクションの開始要求に当たるSYNパケットを大量に送ることによって，攻撃対象のサーバに，接続要求ごとに応答を返すための過大な負荷を掛ける．
エ　大量のTCPコネクションを確立することによって，攻撃対象のサーバに接続を維持させ続けリソースを枯渇させる．

問 11

正解 □ 完璧 □ 直前CHECK □

標準化団体OASISが，Webサイト間で認証，属性及び認可の情報を安全に交換するために策定したフレームワークはどれか．

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問9　ウ

リスク回避とは，リスクが発生しないように事前に対策を行うことである．リスクへの対応方法としては，他に**リスク保有**（受容），**リスク移転**がある．

リスク回避：リスクが発生しないように事前に対策を行うこと

リスク保有（受容）：リスクあることがわかっていても，対策を行わないこと．被害の影響がきわめて小さい場合や，リスクの発生頻度がきわめて低い場合の対応方法である．

リスク移転：保険に入る等により，第三者へ資金的なリスクを移すことである．

ア，イ，エ：リスク保有（受容）に該当する．

ウ：リスク回避に該当する．

問10　ア

ICMP Flood攻撃は，pingを用いてサーバに対して行われる代表的な**DoS**（Denial Of Service:：サービス不能）**攻撃**の一つである．イ，ウ，エの攻撃との違いは，ICMPを利用している点である．利用するプロトコルにより攻撃名称が異なる．

ICMP（Internet Control Message Protocol）：pingやtraceroute（経路情報を得るコマンド）に用いられる送信エラーや，制御メッセージの通知に利用される．

イ：**HTTP GET Flood**の説明である．

ウ：**TCP SYN Flood**の説明である．

エ：**TCP Connection Flood**の説明である．

問11　ア

SAML（Security Assertion Markup Language）：標準化団体OASISによって策定された，IDやパスワードなどの認証情報を安全に交換するための仕様．SAMLを用いることで，一度の認証で複数のWebサイトやサービスの利用が可能となる**シングルサインオン**（SSO：Single Sign-On）を実現できる．WebサイトがSAMLに対応していれば，異なるドメインのサイトへ移動したときに，移動元のサイトと移動先のサイトがSAMLプロトコルで通信し，自動的に認証情報を引き継ぐことができる．

SOAP（Simple Object Access Protocol）：SOAPによる通信では，XML文書にエンベロープと呼ばれる付帯情報がついたメッセージをHTTPなどでやり取りする．

XKMS（XML Key Management Specification）：XMLを利用して公開鍵基盤（PKI）の鍵情報を効率よく管理するためのプロトコルである．

XML Signature：W3C（World Wide Web Consortium）によって勧告された規格．XMLにおいてディジタル署名を利用するための規格である．

問題

問 12

正解 □ 完璧 □ 直前CHECK □

ディジタルフォレンジッ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　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.
エ　犯罪に対する証拠となり得るデータを保全し，その後の訴訟などに備える.

問 13

正解 □ 完璧 □ 直前CHECK □

ゼロデイ攻撃の特徴はどれか.

ア　セキュリティパッチが提供される前にパッチが対象とする脆弱(ぜい)性を攻撃する.
イ　特定のサイトに対し，日時を決めて，複数台のPCから同時に攻撃する.
ウ　特定のターゲットに対し，フィッシングメールを送信して不正サイトへ誘導する.
エ　不正中継が可能なメールサーバを見つけた後，それを踏み台にチェーンメールを大量に送信する.

問 14

正解 □ 完璧 □ 直前CHECK □

SSL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Webサーバのディジタル証明書にはIPアドレスの組込みが必須なので，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.
イ　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.
ウ　SSLはWebサーバを経由した特定の利用者間の通信のために開発されたプロトコルであり，Webサーバ提供者への事前の利用者登録が不可欠である.
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12　エ

ディジタルフォレンジックスは，パソコンやサーバ等のコンピュータ機器が犯罪や裁判での証拠となりえるときに，データを保全し賠償などに備えることや，内容を分析，鑑定するための手段や技術を指す．

ア：**電子透かし**の説明である．

イ：**擬似アタックテスト**の説明である．

ウ：**ソーシャルエンジニアリング**の説明である．

問13　ア

ゼロデイ攻撃とは，ソフトウェアの脆弱性が発見されてからセキュリティパッチが提供されるまでの間に攻撃することである．

イ：**DDoS攻撃**に関する説明である．

ウ：**スピアフィッシング攻撃**に関する説明である．もり（スピア）で魚を突くように特定の相手を攻撃する手法である．

エ：**踏み台攻撃**に関する説明である．

問14　イ

SSL（Secure Socket Layer）は，OSI参照モデルのトランスポート層（第4層）の情報を暗号化して送受信するプロトコルである．暗号化では，複数の共通鍵暗号方式（DESや3DESなど）から使用するものを選択できる．

SSLではサーバやユーザの認証にディジタル証明書を用いる．

ア：SSLを利用するWebサーバ用のディジタル証明書には，一般的にサーバ名やFQDNを組み込むため，IPアドレスを取得する必要はない．

ウ：利用者を登録する必要はない．

エ：制限されていない．128ビット長の共通鍵も広く利用されている．

問題

問 15

正解 完璧 直前CHECK

WAF（Web Application Firewall）のブラックリスト又はホワイトリストの説明のうち，適切なものはどれか．

ア　ブラックリストは，脆弱性があるサイトのIPアドレスを登録したものであり，該当する通信を遮断する．

イ　ブラックリストは，問題がある通信データパターンを定義したものであり，該当する通信を遮断するか又は無害化する．

ウ　ホワイトリストは，暗号化された受信データをどのように復号するかを定義したものであり，復号鍵が登録されていないデータを遮断する．

エ　ホワイトリストは，脆弱性がないサイトのFQDNを登録したものであり，登録がないサイトへの通信を遮断する．

問 16

正解 完璧 直前CHECK

SSLに対するバージョンロールバック攻撃の説明はどれか．

ア　SSLの実装の脆弱性を用いて，通信経路に介在する攻撃者が弱い暗号化通信方式を強制することによって，暗号化通信の内容を解読して情報を得る．

イ　SSLのハンドシェイクプロトコルの終了前で，使用暗号化アルゴリズムの変更メッセージを，通信経路に介在する攻撃者が削除することによって，通信者が暗号化なしでセッションを開始し，攻撃者がセッションの全通信を盗聴したり改ざんしたりする．

ウ　SSLを実装した環境において，攻撃者が物理デバイスから得られた消費電流の情報などを利用して秘密情報を得る．

エ　保守作業のミスや誤操作のときに回復できるようにバックアップしたSSLの旧バージョンのライブラリを，攻撃者が外部から破壊する．

問15　イ

WAF（Web Application Firewall）は，Webアプリケーションのやり取りを把握・管理することによって不正侵入を防御する仕組みをもつファイアウォールである．プログラムに渡される入力内容などを直接検査することによって，不正とみなされたアクセス要求を遮断する仕組みが採用されている．クライアントの操作するWebブラウザとWebサーバの間に介在し，ブラウザとの直接的なやり取りをWAFが受け持つ．SQLインジェクションやクロスサイトスクリプティング，強制ブラウジングといった要求はWAFが遮断する．

ブラックリストには問題のある通信データパターンが定義され，**ホワイトリスト**には問題のない正規の通信データパターンが定義されている．それ以外の通信はいわばグレーゾーンであり，ホワイトリストで許可し，それ以外のグレーゾーンを含む通信を許可するか，ブラックリストのみを拒否してそれ以外のグレーゾーンを含む通信を許可するのかを考えなければならない．

日々新しいWebアプリケーションは増えており，新しい攻撃もあるため，運用面を考慮するとブラックリストとホワイトリストの優劣はつけ難い．

問16　ア

SSLのバージョンロールバック攻撃は，SSL通信経路上の攻撃者により脆弱なバージョンを利用することを強制させられ，情報を盗み取られることである．一般的には，脆弱性のあるバージョンの利用を無効にするなどの対策を取ることで回避可能である．

ウ：**サイドチャネル攻撃**の説明である．

問題

問 17

正解 □ 完璧 □ 直前CHECK □

ネットワークを構成する装置の用途や機能に関する記述のうち，適切なものはどれか．

ア　ゲートウェイは，主にトランスポート層以上での中継を行う装置であり，異なったプロトコル体系のネットワーク間の接続などに用いられる．

イ　ブリッジは，物理層での中継を行う装置であり，フレームのフィルタリング機能をもつ．

ウ　リピータは，ネットワーク層での中継を行う装置であり，伝送途中で減衰した信号レベルの補正と再生増幅を行う．

エ　ルータは，データリンク層のプロトコルに基づいてフレームの中継と交換を行う装置であり，フロー制御や最適経路選択などの機能をもつ．

問 18

正解 □ 完璧 □ 直前CHECK □

DNSSECに関する記述として，適切なものはどれか．

ア　DNSサーバへのDoS攻撃を防止できる．

イ　IPsecによる暗号化通信が前提となっている．

ウ　代表的なDNSサーバの実装であるBINDの代替として使用する．

エ　ディジタル署名によってDNS応答の正当性を確認できる．

問17　ア

ア：**ゲートウェイ**の説明である．
イ：**リピータ**の説明である．
ウ：**ルータ**または**レイヤ3スイッチ**の説明である．
エ：**ブリッジ**または**レイヤ2スイッチ**の説明である

問18　エ

DNSSEC（Domain Name System Security Extension）：DNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を証明するセキュリティ拡張機能．応答を送信するDNSサーバが秘密鍵を使って応答に署名し，受信する側が公開鍵で検証する．秘密鍵で正しい署名を付けるので，署名の検証によって偽の応答を検知できる．

DNSキャッシュポイズニングという，DNSサーバに一時的に保存（キャッシュ）してあるホスト名とIPアドレスの対応情報を偽の情報に書き換える攻撃があり，DNSSECはこの攻撃に対してDNS情報を正しく保つための方法の一つである．DNSキャッシュが不正な情報で汚染されると，クライアントのWebブラウザは偽のWebサイトに誘導されてしまうといったことが起こり，情報漏えいやウイルス感染などの2次的な被害を生じる恐れがある．

問題

問 19

正解 □ 完璧 □ 直前CHECK □

2台のPCをIPv6ネットワークに接続するとき，2台ともプレフィックスが2001:db8:100:1000::/56のIPv6サブネットに入るようになるIPアドレスの組合せはどれか．

	1台目のPC	2台目のPC
ア	2001:db8:100::aa:bb	2001:db8:100::cc:dd
イ	2001:db8:100:1000:aa:bb	2001:db8:100:2000:cc:dd
ウ	2001:db8:100:1010:aa:bb	2001:db8:100:1020:cc:dd
エ	2001:db8:100:1100:aa:bb	2001:db8:100:1200:cc:dd

問 20

正解 □ 完璧 □ 直前CHECK □

HTTPの認証機能を利用するクライアント側の処理として，適切なものはどれか．

ア　ダイジェスト認証では，利用者IDとパスワードを“:”で連結したものを，MD5を使ってエンコードしAuthorizationヘッダで指定する．

イ　ダイジェスト認証では，利用者IDとパスワードを“:”で連結したものを，SHAを使ってエンコードしAuthorizationヘッダで指定する．

ウ　ベーシック認証では，利用者IDとパスワードを“:”で連結したものを，BASE64でエンコードしAuthorizationヘッダで指定する．

エ　ベーシック認証では，利用者IDとパスワードを“:”で連結したものを，エンコードせずにAuthorizationヘッダで指定する．

問19　ウ

IPv6のIPアドレス長は128ビットとなっている．表記方法は，16ビット単位に「:（コロン）」で区切る形である．RFC5952では，表記ルールの0の省略方法を示している．本問もそのルールに従って省略されている点を読み取る必要がある．

① 16ビットの「:」区切りの先頭にある0は省略する

例　2001:0db8:0100 = 2001:db8:100

② 0000が連続する場合は「::」を使用して可能な限り省略する．

③ 0000が1箇所しかない場合「::」使用して省略してはならない．

④ 「::」を使用して省略可能な箇所が複数ある場合は，最も多くの0を省略できる箇所を省略する．ただし，省略できる0の数が複数の個所で同じ場合は，先の0を省略する．

本問には「/56」という表記があるから，左側の先頭から56ビットがサブネットワークとなる．

設問の「2001:db8:100:1000::/56」の56ビット分を省略しない形に変換すると，以下のようになる．

省略前	2001:0db8:0100:10

選択肢ウのPCは，省略前のサブネットと一致する組合せとなる．

問20　ウ

HTTPのダイジェスト認証：ユーザ名とパスワードを利用したランダムな文字列をMD5でエンコードして，サーバで認証する仕組みである．

HTTPのベーシック認証：利用者IDとパスワードをBASE64でエンコードして，サーバへ送信し，認証する仕組みである．

ア：ユーザIDとパスワードをそのままMD5でエンコードするのではない．

イ：SHAは利用しない．

エ：何もエンコードしないのは誤りである．

問題

問 21

正解 完璧 直前CHECK

データベースのデータを更新するトランザクションが，実行途中で異常終了したとき，更新中のデータに対して行われる処理はどれか．

ア　異常終了時点までの更新ログ情報を破壊することによって，データをトランザクション開始前の状態に回復する．
イ　チェックポイント時点からコミットが完了しているトランザクションの更新をロールフォワードすることによって，データを回復する．
ウ　トランザクションの更新ログ情報を使って異常終了時点までロールフォワードすることによって，データを回復する．
エ　ロールバックすることによって，データをトランザクション開始前の状態に回復する．

問 22

正解 完璧 直前CHECK

オブジェクト指向における情報隠蔽に関する記述として，適切なものはどれか．

ア　オブジェクトの特性（属性，関連，操作）をまとめて抽象化する．
イ　オブジェクトは，メッセージによってだけアクセス可能となる．
ウ　親クラスに定義されたメソッドを，実行時に子クラスに引き継ぐ．
エ　同一メッセージでも，実行時の受信クラスに基づいて適用されるメソッドが決まる．

問 23

正解 完璧 直前CHECK

特許権に関する記述のうち，適切なものはどれか．

ア　A社が特許を出願するよりも前に独自に開発して発売した商品は，A社の特許権の侵害にならない．
イ　組込み機器におけるハードウェアは特許権で保護されるが，ソフトウェアは保護されない．
ウ　審査を受けて特許権を取得した後に，特許権が無効となることはない．
エ　先行特許と同一の技術であっても，独自に開発した技術であれば特許権の侵害にならない．

問21　エ

データベースを更新するトランザクションが異常終了したときは，そのトランザクションの実行を取り消すことが必要になる．これを**後退復帰（ロールバック）**と呼ぶ．

システム障害の発生に対応するためには，チェックポイントが用いられる．ある時点での更新情報をデータベース本体に反映させたものが**チェックポイント**である．それ以降の更新は，処理効率を配慮したタイミングでデータベース本体に反映される．システム障害が発生すると，すでに終了しているトランザクションであれば**ロールフォワード**が実行され，処理を完了させる．まだ完了していないトランザクションはロールバックされる．

問22　イ

オブジェクト指向では情報の隠蔽を**カプセル化**と呼ぶ．具体的には，モジュールを外部から隔離し，ブラックボックス化することである．カプセル化したモジュールは関数だけをモジュール外に公開して，メッセージのみをアクセス可能とする．

ウ：**インヘリタンス**の説明である．

問23　ア

特許権は，産業上，利用することができる新規の発明（自然法則を利用した技術的思想の創作）を独占的・排他的に利用できる権利であり，所轄の官庁への出願及び審査に基づいて付与される権利である．権利の存続期間は出願の日から20年である．

ア：特許出願前から販売している製品には**先使用権**が認められる．先使用権とは，もともと利用されていた技術は他人の特許出願によっても利用を継続できる権利である．

イ：平成14年の法改正で，ソフトウェアの特許が認められた．

ウ：特許取得後であっても，その特許が無効と判定されることもある．

エ：先行特許に対する権利侵害になる．

問 24

正解 完璧 直前CHECK

ソフトウェア開発・保守の工程において，リポジトリを構築する理由として，最も適切なものはどれか．

ア　各工程で検出した不良を管理することが可能になり，ソフトウェアの品質分析が容易になる．

イ　各工程での作業手順を定義することが容易になり．開発・保守時の作業ミスを防止することができる．

ウ　各工程での作業予定と実績を関連付けて管理することが可能になり，作業の進捗管理が安易になる．

エ　各工程での成果物を一元管理することによって，開発・保守作業の効率が良くなり，用語の統一もできる．

問 25

正解 完璧 直前CHECK

システム監査で用いる統計的サンプリングに関する記述のうち，適切なものはどれか．

ア　開発プロセスにおけるコントロールを評価する際には，開発規模及び影響度の大きい案件を選定することによって，母集団全体への評価を導き出すことができる．

イ　コントロールが有効であると判断するために必要なサンプル件数を事前に決めることができる．

ウ　正しいサンプリング手順を踏むことによって，母集団全件に対して検証を行う場合と同じ結果を常に導き出すことができる．

エ　母集団からエラー対応が行われたデータを選定することによって，母集団全体に対してコントロールが適切に行われていることを確認できる．

問24　エ

リポジトリは，システム開発で用いるファイルやドキュメントなど，各工程での生産物を一元的に管理するためのものである．

ア：リポジトリに品質管理機能はない．

イ：リポジトリは作業手順を定義するものではない．

ウ：リポジトリに作業の予定・実行管理機能はない．

問25　イ

統計的サンプリングの原則は，無作為抽出である．**サンプリング**は監査テーマあるいはその目的から，母集団定義，許容誤差水準決定，サンプル数算出・抽出法（単純無作為，系統（等間隔）抽出，多段抽出，層別抽出等）を選択し，乱数表等を用いて標本を母集団からランダムに抽出する．