問 1 正解 完璧 直前チェック

AESの暗号化方式を説明したものはどれか。

ア　鍵長によって，段数が決まる。
イ　段数は，6回以内の範囲で選択できる。
ウ　データの暗号化，復号，暗号化の順に3回繰り返す。
エ　同一の公開鍵を用いて暗号化を3回繰り返す。

問 2 正解 完璧 直前チェック

特定の認証局が発行したCRLに関する記述のうち，適切なものはどれか。

ア　CRLには，失効したディジタル証明書に対応する秘密鍵が登録される。
イ　CRLには，有効期限内のディジタル証明書のうち失効したディジタル証明書と失効し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　有効期限切れで失効したディジタル証明書は，所有者が新たなディジタル証明書を取得するまでの間，CRLに登録される。

問 3 正解 完璧 直前チェック

ステートフルインスペクション方式のファイアウォールの特徴はどれか。

ア　Webブラウザと Webサーバとの間に配置され，リバースプロキシサーバとして動作する方式であり，Webブラウザから Webサーバへの通信に不正なデータがないかどうかを検査する。
イ　アプリケーションプロトコルごとにプロキシプログラムを用意する方式であり，クライアントからの通信を目的のサーバに中継する際に，不正なデータがないかどうかを検査する。
ウ　特定のアプリケーションプロトコルだけを通過させるゲートウェイソフトウェアを利用する方式であり，クライアントからのコネクションの要求を受け付けて，目的のサーバに改めてコネクションを要求することによって，アクセスを制御する。
エ　パケットフィルタリングを拡張した方式であり，過去に通過したパケットから通信セッションを認識し，受け付けたパケットを通信セッションの状態に照らし合わせて通過させるか遮断させるかを判断する。

問1　ア

解説　**AES**（Advanced Encryption Standard）は，米国政府標準の**共通鍵暗号方式**である。

共通鍵暗号方式は，**暗号化鍵**と**復号鍵**に同じ鍵を使用するため，鍵を共有する手続きが必要である。

鍵長は128ビット，192ビット，256ビットの選択が可能なSPN型ブロック暗号である。ブロック長は128ビットとなっている。**SPN型ブロック暗号**とは，換字と転置を繰り返す暗号方式で，これを「段」と呼ぶ複数回の繰り返しによって暗号化の強度を上げる方式である。

問2　イ

解説　**CRL**（Certificate Revocation List）は，有効期間中に失効した公開鍵証明書のリストで，認証局から発行される。公開鍵証明書の検証時に，公開鍵証明書の失効確認に使用するため常に参照される。

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，公開鍵が登録される。
ウ：CRLは定期的に更新されるがリアルタイムに更新されない。
エ：失効したディジタル証明書は，所有者が新たなディジタル証明書を取得してもCRLに登録された状態を継続する。

問3　エ

解説　**ステートフルインスペクション方式**は，ファイアウォールを通過したパケットの通信セッションを認識し，通信セッションの状態に合わせて通過させる方式である。

例えば，あるソフトウェアのデータ通信時に制御用通信とデータ転送用通信を別々のポートで通信する場合，ステートフルインスペクション方式であれば，制御用の通信がファイアウォールを通過したときに，動的にデータ転送用通信ポートを開放する。通常はファイアウォールで遮断しているポートが必要に応じて開放される仕組みである。

ア：**WAF**（Web Application Firewall）の説明である。
イ，ウ：アプリケーションゲートウェイ方式の説明である。

問 4 正解 完璧 直前チェック

PCなどに内蔵されるセキュリティチップ（TPM：Trusted Platform Module）がもつ機能はどれか。

ア　TPM間での共通鍵の交換　　イ　鍵ペアの生成
ウ　ディジタル証明書の発行　　エ　ネットワーク経由の乱数送信

問 5 正解 完璧 直前チェック

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　感染するごとにウイルスのコードを異なる鍵で暗号化し，コード自身を変化させることによって，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 6 正解 完璧 直前チェック

ISO/IEC 15408を評価基準とする“ITセキュリティ評価及び認証制度”の説明として，適切なものはどれか。

ア　暗号モジュールに暗号アルゴリズムが適切に実装され，暗号鍵などが確実に保護されているかどうかを評価及び認証する制度
イ　主に無線LANにおいて，RADIUSなどと連携することで，認証されていない利用者を全て排除し，認証された利用者だけの通信を通過させることを評価及び認証する制度
ウ　情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する制度
エ　情報セキュリティマネジメントシステムが，基準にのっとり，適切に組織内に構築，運用されていることを評価及び認証する制度

問4　イ

解説 **TPM**とは，PCに内蔵する暗号化の鍵を格納するセキュリティチップである。一般的に，企業向けPCのハードディスクを暗号化してセキュリティを高めるために，このチップの搭載が進んでいる。

仕組みとしては，ハードディスクを暗号化する鍵をセキュリティチップに記録する。ハードディスクが盗難にあってもセキュリティチップに格納された鍵がなければ複合できない。

セキュリティチップには，ハードディスクに格納するデータを暗号化するための鍵を生成する機能がある。

ア：TPM間の共通鍵ではなく，TPMとハードディスク間の共通鍵交換となる。
ウ：証明書の発行は，TPMでは行えない。
エ：TPMはPC内のみで利用できる。PCから外すとPCが起動できなくなる。したがって，取り外しやネットワーク経由などでは利用できない。

問5　イ

解説 **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：ボットの説明である。
ウ：マルチプラットフォーム型ウイルスの説明である。
エ：ステルス型ウイルスの説明である。

問6　ウ

解説 ISO/IEC 15408は，CC（Common Criteria）と呼ばれ，情報技術セキュリティの観点から，情報技術に関連した製品及びシステムが適切に設計され，その設計が正しく実装されていることを評価するための国際標準規格である。情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する。

ア：暗号モジュール試験及び認証制度の説明である。
イ：この選択肢の内容となる制度はない。
エ：情報セキュリティマネジメントシステム（JIS Q 27001：ISMS）認証制度の説明である。

問 7 正解 完璧 直前チェック

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 8 正解 完璧 直前チェック

水飲み場型攻撃（Watering Hole Attack）の手口はどれか。

ア　アイコンを文書ファイルのものに偽装した上で，短いスクリプトを埋め込んだショートカットファイル（LNKファイル）を電子メールに添付して標的組織の従業員に送信する。
イ　事務連絡などのやり取りを行うことで，標的組織の従業員の気を緩めさせ，信用させた後，攻撃コードを含む実行ファイルを電子メールに添付して送信する。
ウ　標的組織の従業員が頻繁にアクセスするWebサイトに攻撃コードを埋め込み，標的組織の従業員がアクセスしたときだけ攻撃が行われるようにする。
エ　ミニブログのメッセージにおいて，ドメイン名を短縮してリンク先のURLを分かりにくくすることによって，攻撃コードを埋め込んだWebサイトに標的組織の従業員を誘導する。

問 9 正解 完璧 直前チェック

不正が発生する際には“不正のトライアングル”の3要素全てが存在すると考えられている。“不正のトライアングル”の構成要素の説明のうち，適切なものはどれか。

ア　“機会”とは，情報システムなどの技術や物理的な環境及び組織のルールなど，内部者による不正行為の実行を可能，又は容易にする環境の存在である。
イ　“情報と伝達”とは，必要な情報が識別，把握及び処理され，組織内外及び関係者相互に正しく伝えられるようにすることである。
ウ　“正当化”とは，ノルマによるプレッシャーなどのことである。
エ　“動機”とは，良心のかしゃくを乗り越える都合の良い解釈や他人への責任転嫁など，内部者が不正行為を自ら納得させるための自分勝手な理由付けである。

問7　ウ

解説　リスク対応には，リスク回避，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）：リスクが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：保険に入るなどにより，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8　ウ

解説　**水のみ場型攻撃**は，標的型攻撃の一種で，特定の組織や個人をターゲット（標的）として，そのターゲットが頻繁にアクセスするWebサイトを改ざんし，アクセスした際にウイルスやマルウェアを感染させる。水のみ場に集まる動物を狙う猛獣に例えた攻撃手法である。
ア，イ，ウ：標的型攻撃の説明である。

問9　ア

解説　**不正のトライアングル**とは，米国の犯罪学者D.R.クレッシーが提唱した，人が不正行為を実現化するときの理論である。不正行為は，①機会，②動機，③正当化が揃ったときに実行される。逆にこの三つが揃わないと不正は起きない。
機会：不正行為の実行が可能となる環境。
動機：不正行為を実行しなければならない事情。
正当化：不正行為を肯定する理由付けがされた常態。
イ：不正のトライアングルには該当しない理由である。
ウ：動機の説明である。
エ：正当化の説明である。

問 10 正解 完璧 直前チェック

ICMP Flood攻撃に該当するものはどれか。

ア　HTTP GETコマンドを繰り返し送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける。
イ　pingコマンドを用いて大量の要求パケットを発信することによって，攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する。
ウ　コネクション開始要求に当たる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てリソースを枯渇させる。

問 11 正解 完璧 直前チェック

VLAN機能をもった1台のレイヤ3スイッチに複数のPCを接続している。スイッチのポートをグループ化して複数のセグメントに分けると，セグメントを分けない場合に比べて，どのようなセキュリティ上の効果が得られるか。

ア　スイッチが，PCから送出されるICMPパケットを全て遮断するので，PC間のマルウェア感染のリスクを低減できる。
イ　スイッチが，PCからのブロードキャストパケットの到達範囲を制限するので，アドレス情報の不要な流出のリスクを低減できる。
ウ　スイッチが，PCのMACアドレスから接続可否を判別するので，PCの不正接続のリスクを低減できる。
エ　スイッチが，物理ポートごとに，決まったIPアドレスのPC接続だけを許可するので，PCの不正接続のリスクを低減できる。

問10　イ

解説　**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。ア，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。

ア：**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　イ

解説　**レイヤ3スイッチ**は，OSI基本参照モデルのネットワーク層（ルーティング）通信に利用されるスイッチングハブである。ネットワーク層では，セグメント単位にデータリンク層でのブロードキャストパケットの到達範囲を制限することができる。セグメントは，サブネットマスクで指定された同一のネットワークとなる。言い換えると，セグメントは，ルーティングしない範囲での通信ともいえる。

ア：ICMPパケットは通常遮断されない。パケットフィルタなど明示的に設定した場合のみ遮断できる。
ウ：レイヤ3スイッチの標準的な利用では，PCのMACアドレスから接続可否を判断することはない。
エ：物理ポートごとのPC接続だけを許可することは，レイヤ3スイッチの標準機能では実施されない。

問 12 正解 完璧 直前チェック

クロスサイトスクリプティングによる攻撃を防止する対策はどれか。

ア　WebサーバにSNMPエージェントを常駐稼働させ，Webサーバの負荷状態を監視する。
イ　WebサーバのOSのセキュリティパッチについて，常に最新のものを適用する。
ウ　Webサイトへのデータ入力について，許容範囲を超えた大きさのデータの書込みを禁止する。
エ　Webサイトへの入力データを表示するときに，HTMLで特別な意味をもつ文字のエスケープ処理を行う。

問 13 正解 完璧 直前チェック

WebサーバがHTTPS通信の応答でCookieにSecure属性を設定したときのブラウザの処理はどれか。

ア　ブラウザは，Cookieの“Secure =”に続いて指定された時間を参照し，指定された時間を過ぎている場合にそのCookieを削除する。
イ　ブラウザは，Cookieの“Secure =”に続いて指定されたホスト名を参照し，指定されたホストにそのCookieを送信する。
ウ　ブラウザは，Cookieの“Secure”を参照し，HTTPS通信時だけそのCookieを送信する。
エ　ブラウザは，Cookieの“Secure”を参照し，ブラウザの終了時にそのCookieを削除する。

問 14 正解 完璧 直前チェック

テンペスト（TEMPEST）攻撃を説明したものはどれか。

ア　故意に暗号化演算を誤動作させて正しい処理結果との差異を解析する。
イ　処理時間の差異を計測し解析する。
ウ　処理中に機器から放射される電磁波を観測し解析する。
エ　チップ内の信号線などに探針を直接当て，処理中のデータを観測し解析する。

問12　エ

解説　**クロスサイトスクリプティング**は，動的にWebページを生成するアプリケーションの脆弱性を利用した攻撃である。例えば，攻撃者によって掲示板に悪意のスクリプトコードが書き込まれた場合に，スクリプトコードをチェックせずに掲示板に載せることで，その掲示板にアクセスしたブラウザが悪意のスクリプトを実行する。対策としては，入力されたデータをチェックして，スクリプトの文字列を置き換えて無効化する**サニタイジング**が有効である。

ア：SNMPで負荷状態を監視することは，システムの稼動に関する監視である。クロスサイトスクリプティングによる攻撃を防ぐことはできない。
イ：OSのセキュリティパッチは，外部からの攻撃に有効であるが，クロスサイトスクリプティングによる攻撃を防ぐことはできない。
ウ：データ入力の許容範囲を超えたものは容量の問題であって，クロスサイトスクリプティングによる攻撃を防ぐことはできない。

問13　ウ

解説　WebサーバがHTTPS通信を利用している場合，セッションIDが第三者に漏えいすることを防止するために，cookie発行時にSecure属性を付ける対策がある。これは，Webへのアクセスの際に同一ホスト内で，HTTPのページとHTTPSのページがあり，相互に行き来する場合にHTTP通信時にHTTPSで使うべきcookieの値が流出する可能性があるためである。対処方法としては，HTTPS通信時だけcookieを送信する。

問14　ウ

解説　**テンペスト攻撃**とは，コンピュータやディスプレイ，ケーブルなどから放射される電磁波を受信・解析することで，キー入力情報の収集や表示画面の復元などを行う攻撃（盗聴）手法である。

テンペスト攻撃の対策としては，周辺機器やケーブルなどをシールドして電波の放射を防ぐ方法が有効である。具体的には，回線設計の段階で信号の漏えいを防ぎつつ，ケーブルなどを被覆して電磁波をシールドすることが基本的な対策である。また，コンピュータの設置された部屋全体をシールドする手段もある。

問 15 正解 完璧 直前チェック

脆弱性検査で，対象ホストに対してポートスキャンを行った。対象ポートの状態を判定する方法のうち，適切なものはどれか。

ア　対象ポートにSYNパケットを送信し，対象ホストから“RST/ACK”パケットを受信するとき，接続要求が許可されたと判定する。
イ　対象ポートにSYNパケットを送信し，対象ホストから“SYN/ACK”パケットを受信するとき，接続要求が中断又は拒否されたと判定する。
ウ　対象ポートにUDPパケットを送信し，対象ホストからメッセージ“port unreachable”を受信するとき，対象ポートが閉じていると判定する。
エ　対象ポートにUDPパケットを送信し，対象ホストからメッセージ“port unreachable”を受信するとき，対象ポートが開いていると判定する。

問 16 正解 完璧 直前チェック

ダウンローダ型マルウェアが内部ネットワークのPCに感染したとき，そのマルウェアによってインターネット経由で他のマルウェアがダウンロードされることを防ぐ対策として，最も有効なものはどれか。

ア　URLフィルタを用いてインターネット上の危険なWebサイトへの接続を遮断する。
イ　インターネットから内部ネットワークに向けた要求パケットによる不正侵入行為をIPSで破棄する。
ウ　スパムメール対策サーバでインターネットからのスパムメールを拒否する。
エ　メールフィルタで他サイトへの不正メール発信を遮断する。

問 17 正解 完璧 直前チェック

OAuth 2.0において，WebサービスAの利用者Cが，WebサービスBにリソースDを所有している。利用者Cの承認の下，WebサービスAが，リソースDへの限定的なアクセス権限を取得するときのプロトコルOAuth 2.0の動作はどれか。

ア　WebサービスAが，アクセストークンを発行する。
イ　WebサービスAが，利用者Cのディジタル証明書をWebサービスBに送信する。
ウ　WebサービスBが，アクセストークンを発行する。
エ　WebサービスBが，利用者Cのディジタル証明書をWebサービスAに送信する。

問15　ウ

解説　ポートスキャンの結果から状態を判定する場合，TCPとUDP両方のポートが開いている場合と閉じている場合の動作を理解する必要がある。

ア：**RST/ACK（リセット）**が返信された場合は，ポートは閉じていると判断する。RST/ACKは，通信を拒否されたときに返信されるパケットである。

イ：**SYN/ACK（応答）**が返信された場合は，ポートは開いていると判断する。SYN/ACKは，通信を許可されたパケットである。

ウ，エ：**port unreachable（ポート到達不可）**は，ポートが閉じている場合に受信するパケットである。

問16　ア

解説　**マルウェア**は，外部からPCに進入するコンピュータウイルスである。PCの破壊や，情報の漏えいなどを行う有害ソフトウェアである。マルウェアに感染したPCは，インターネットの有害サイトへ自動接続し，他のマルウェアをダウンロードするなどを行う。対策としてはURLフィルタを用いることで，インターネット上の危険なサイトとPCの通信を遮断できる。

イ：インターネットから内部ネットワーク向けのパケットをブロックすることと，内部のマルウェアがダウンロードすることは関連していない。

ウ：スパムメールの拒否と，マルウェアの動作は関連してない。

エ：マルウェアはメールではなく，インターネットとの直接通信を行う。したがって不正メール発信とは関連しない。

問17　ウ

解説　**OAuth2.0**とは，利用者へのWebサービスアクセス権を，利用者の代理で許可するための認証用プロトコルである。OAuthを利用すると，利用者は認証の際にユーザ名やパスワードをコンテンツ提供者に知らせることなくアクセス許可認証を行うことができる。

WebサービスAが認証を取得する場合は，リソースを所有しているWebサービスBがアクセストークンを発行する。

問 18 正解 完璧 直前チェック

DNSのMXレコードで指定するものはどれか。

ア　宛先ドメインへの電子メールを受け付けるメールサーバ
イ　エラーが発生したときの通知先のメールアドレス
ウ　複数のDNSサーバが動作しているときのマスタDNSサーバ
エ　メーリングリストを管理しているサーバ

問 19 正解 完璧 直前チェック

スパニングツリープロトコルの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(うかい)ルート決定を行う。

問 20 正解 完璧 直前チェック

ファイル転送プロトコルTFTPをFTPと比較したときの記述として，適切なものはどれか。

ア　暗号化を用いてセキュリティ機能を強化したファイル転送プロトコル
イ　インターネットからのファイルのダウンロード用に特化したファイル転送プロトコル
ウ　テキストデータの転送を効率的に行うためにデータ圧縮機能を追加したファイル転送プロトコル
エ　ユーザ認証を省略しUDPを用いる，簡素化されたファイル転送プロトコル

問18　ア

解説　**DNS**（Domain Name System）で利用されるデータを，リソースレコード（RR）と呼ぶ。主なリソースレコードの役割は以下のとおりである。

レコード名	説明
MXレコード （Mail Exchangerレコード）	電子メールの送信に利用される。DNS上で電子メールの配送先ホスト名を指定する際に利用する。
NSレコード （Name Serverレコード）	ドメインの委任を行うときに指定するレコード。例えばxxx.co.jpというドメインを立ち上げたときに co.jp から各種レコードを参照するため，co.jp側にてxxx.co.jpのNSレコードを設定する必要がある。
PTRレコード （逆引きレコード）	IPアドレスからドメイン名を問い合わせるためのレコード。
SOAレコード （Start Of Authorityレコード）	DNSで指定するゾーン（xxx.co.jp）の基本的な設定を行うレコード。シリアル，リフレッシュなどを指定する。
Aレコード （正引きレコード）	ドメイン名からIPアドレスを問い合わせるためのレコード。
CNAMEレコード （Canonical Nameレコード）	ホスト名に別名を付けるレコード。

問19　エ

解説　LANにおいてループ状の構成がある場合，データがネットワーク上にとどまり続けることがある。これをループと呼び，このループを回避するためのプロトコルが**スパニングツリープロトコル**である。
ア，イ：レイヤ2スイッチングハブの機能である。
ウ：ロードバランサの機能である。

問20　エ

解説
TFTP（Trivial File Transfer Protocol）：UDPによるファイル転送プログラムで，FTPと比較して簡易機能となっている。
FTP（File Transfer Protocol）：インターネットなどのTCP/IP環境でファイルを転送する際に使われるプロトコルである。
ア：ftp，tftpでは，暗号化されない。
イ：インターネットのファイルダウンロード用に特化したものではない。
ウ：テキストデータだけでなく，バイナリデータの転送も可能である。

問 21 正解 完璧 直前チェック

データウェアハウスを構築するために，業務システムごとに異なっているデータ属性やコード体系を統一する処理はどれか。

ア　ダイス　　イ　データクレンジング
ウ　ドリルダウン　　エ　ロールアップ

問 22 正解 完璧 直前チェック

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，作業の進捗管理が容易になる。
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 23 正解 完璧 直前チェック

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B社が独自に開発して日本国内で発売した製品は，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　イ

解説 **OLAP**（OnLine Analytical Processing）の操作に関する設問である。OLAPは，データベースなどに蓄積されたデータを多次元的に解析するシステムである。
ダイス：分析軸を入れ替えてデータの切り口を変えることである。
データクレンジング：データベースにおいて，既存のデータを最適かつ整合性のある状態に修正する作業や処理である。顧客管理データベースにおいて，重複する顧客情報を一本化する作業，市町村の合併に対応した住所整備の作業などがある。
ドリルダウン：集計単位をより小さくする操作のことである。
ロールアップ：集計単位をより大きくする操作のことである。

問22　エ

解説 **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23　ア

解説 **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およ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のことである。
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：特許権の存続期間は20年である。
エ：先行特許に対する権利侵害になる。

問 24 正解 完璧 直前チェック

入出力データの管理方針のうち，適切なものはどれか。

ア　出力帳票の受渡しは授受管理表などを用いて確実に行い，情報の重要度によっては業務部門の管理者に手渡しする。

イ　出力帳票の利用状況を定期的に点検し，利用されていないと判断したものは，情報システム部門の判断で出力を停止する。

ウ　チェックによって発見された入力データの誤りは，情報システム部門の判断で修正する。

エ　入力原票やEDI受信ファイルなどの取引情報は，機密性を確保するために，データをシステムに取り込んだら速やかに廃棄する。

問 25 正解 完璧 直前チェック

システム監査における監査証拠の説明のうち，適切なものはどれか。

ア　監査人が収集又は作成する資料であり，監査報告書に記載する監査意見や指摘事項は，その資料によって裏付けられていなければならない。

イ　監査人が当初設定した監査手続を記載した資料であり，監査人はその資料に基づいて監査を実施しなければならない。

ウ　機密性の高い情報が含まれている資料であり，監査人は監査報告書の作成後，速やかに全てを処分しなければならない。

エ　被監査部門が監査人に提出する資料であり，監査人が自ら作成する資料は含まれない。

問24　ア

解説　入出力データの管理方針では，出力帳票やデータの管理などを確実に行う必要がある。

イ，ウ，：情報システム部門の判断ではなく，業務部門の判断となる。情報システム部門は，システムを担当するためデータの判断は行わない。

エ：入力ミスなどを考慮することや確証のために，廃棄せず決められた期間，入力原票を保管しておく必要がある。

問25　ア

解説　**監査証拠**は，監査業務の全過程において監査人が収集および作成した資料である。監査意見や指摘事項の確証となるもので，ヒアリングの結果やシステムの検証結果などが該当する。

イ：監査計画の説明である。

ウ：機密性の高い情報は含まれているが，報告書と合わせて証拠も提出する必要がある。

エ：監査人が被監査人に提出する資料であり，意味が逆である。