問 1 正解 完璧 直前チェック

CRL（Certificate Revocation List）に掲載されるものはどれか。

ア　有効期限切れになったディジタル証明書の公開鍵
イ　有効期限切れになったディジタル証明書のシリアル番号
ウ　有効期限内に失効したディジタル証明書の公開鍵
エ　有効期限内に失効したディジタル証明書のシリアル番号

問 2 正解 完璧 直前チェック

PKIを構成するOCSPを利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。
イ　ディジタル証明書から生成した鍵情報の交換がOCSPクライアントとレスポンダの間で失敗した際，認証状態を確認する。
ウ　ディジタル証明書の失効情報を問い合わせる。
エ　有効期限が切れたディジタル証明書の更新処理の進捗状況を確認する。

問 3 正解 完璧 直前チェック

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1　エ

解説 **CRL**は，有効期限内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，公開鍵証明書が失効しているかどうかを確認できる。

公開鍵証明書の有効期限内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。

問2　ウ

解説 **OCSP**（Online Certificate Status Protocol）は，ディジタル証明書の失効情報をリアルタイムで確認するためのプロトコルである。OCSPはCRL（証明書失効リスト）の代替として策定され，CRLをもたなくてもリアルタイムで失効情報を確認することが可能である。RFC 2560によって規定されている。

問3　ア

解説

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 4 正解 完璧 直前チェック

ハッシュ関数の性質の一つである衝突発見困難性に関する記述のうち，適切なものはどれか。

ア　SHA-256の衝突発見困難性を示す，ハッシュ値が一致する二つのメッセージの探索に要する最大の計算量は，256の2乗である。
イ　SHA-256の衝突発見困難性を示す，ハッシュ値の元のメッセージの探索に要する最大の計算量は，2の256乗である。
ウ　衝突発見困難性とは，ハッシュ値が与えられたときに，元のメッセージの探索に要する計算量が大きいことによる，探索の困難性のことである。
エ　衝突発見困難性とは，ハッシュ値が一致する二つのメッセージの探索に要する計算量が大きいことによる，探索の困難性のことである。

問 5 正解 完璧 直前チェック

情報セキュリティにおけるエクスプロイトコードの説明はどれか。

ア　同じセキュリティ機能をもつ製品に乗り換える場合に，CSVなど他の製品に取り込むことができる形式でファイルを出力するプログラム
イ　コンピュータに接続されたハードディスクなどの外部記憶装置や，その中に保存されている暗号化されたファイルなどを閲覧，管理するソフトウェア
ウ　セキュリティ製品を設計する際の早い段階から実際に動作する試作品を作成し，それに対する利用者の反応を見ながら徐々に完成に近づける開発手法
エ　ソフトウェアやハードウェアの脆弱(ぜい)性を利用するために作成されたプログラム

問4　エ

解説　**衝突発見困難性**は，ハッシュ値が一致する二つのメッセージを探索するための計算量が大きいことによって，探索が困難となり解読されにくいことを意味する。ハッシュ値はあらかじめわかっていない状態から解析を行う。

問5　エ

解説　**エクスプロイトコード**(exploit code)とは，ソフトウェアのセキュリティホールを利用して，不正な動作を再現するプログラムである。たとえば，OSのセキュリティホールを利用して，特権アカウントを搾取するプログラムなどが該当する。
ア：CSVなどほかの製品が取り込める形式でのファイル出力は，エクスポートと呼ばれる。
イ：エクスプロイトコードは，暗号化を解除するものではない。
ウ：試作品を作成し，利用者の反応を見ながら完成形に近づける開発手法は，プロトタイプモデルとなる。

問 6 正解 完璧 直前チェック

DNSに対するカミンスキー攻撃（Kaminsky's attack）への対策はどれか

ア　DNSキャッシュサーバと権威DNSサーバとの計2台の冗長構成とすることによって，過負荷によるサーバダウンのリスクを大幅に低減させる。
イ　SPF（Sender Policy Framework）を用いてMXレコードを認証することによって，電子メールの送信元ドメインが詐称されていないかどうかを確認する。
ウ　問合せ時の送信元ポート番号をランダム化することによって，DNSキャッシュサーバに偽の情報がキャッシュされる確率を大幅に低減させる。
エ　プレースホルダを用いたエスケープ処理を行うことによって，不正なSQL構文によるDNSリソースレコードの書換えを防ぐ。

問 7 正解 完璧 直前チェック

DoS攻撃の一つであるSmurf攻撃はどれか。

ア　ICMPの応答パケットを攻撃対象に大量に送り付ける。
イ　TCP接続要求であるSYNパケットを攻撃対象に大量に送り付ける。
ウ　サイズが大きいUDPパケットを攻撃対象に大量に送り付ける。
エ　サイズが大きい電子メールや大量の電子メールを攻撃対象に送り付ける。

問 8 正解 完璧 直前チェック

暗号化装置において暗号化処理時に消費電力を測定するなどして，当該装置内部の秘密情報を推定する攻撃はどれか。

ア　キーロガー　　イ　サイドチャネル攻撃
ウ　スミッシング　　エ　中間者攻撃

問6　ウ

解説　DNSに対する**カミンスキー攻撃**は，攻撃対象のDNSサーバに対して，存在するURLと同じドメイン内の存在しない名前を連続的に検索させDNSキャッシュを汚染させる攻撃である。カミンスキーとは，この攻撃手法を発見した，ダン・カミンスキー氏から取られた名称である。

カミンスキー攻撃への対策は，DNSでの問合せ時に使用する送信元ポート番号をランダム化することでDNSキャッシュサーバに偽の情報がキャッシュされる確率を大幅に低減させることである。

ア：カミンスキー攻撃はキャッシュを汚染させる攻撃であるため，冗長化構成では対策とならない。
イ：電子メールで利用するMXレコードの対策では，IPアドレス情報をキャッシュするカミンスキー攻撃対策とはならない。
エ：説明文は，SQLインジェクションの対策である。

問7　ア

解説　**Smurf攻撃**とは，ネットワークに大量のパケットを発生させてサービス不能状態を作り出す攻撃手法である。ICMPでは，ICMP Echo Requestが送信されるとEcho Replayが返信される。攻撃者は送信元を攻撃対象のサイトに偽造して，Echo Requestをブロードキャストアドレス宛に送信する。Echo Replyがネットワークのすべてのコンピュータから返信され，この大量のReplyによりサービス不能となる。

問8　イ

解説

キーロガー：コンピュータへのキー入力をすべて記録して，パスワード等を入手する目的で利用される。不特定多数で利用されるPCへ仕掛けることで，ネットバンキングの口座番号や暗証番号などを盗むことに利用される場合が多い。

サイドチャネル攻撃：暗号を解読するための攻撃手法の一つである。暗号化や復号をする際に発生する電磁波，熱，演算処理時間など暗号化を直接解読するのではなく，外部からの観測といった二次的要素から解読を行う手法である。

スミッシング：携帯電話のSMS（ショートメッセージングサービス）を利用してあたかも有名サイトや，携帯会社のふりをし，フィッシングサイトに誘導する詐欺手法である。

中間者攻撃（Man-in-the-middle）：通信を行う2者間に割り込んで，両者が交換する情報を自分のものとすり替えることによって，気づかれることなくデータを盗聴する。

問 9 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クライアントと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クライアントからの通信を目的のWebサーバに中継する際に，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ソフトウェア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，通信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するかを判断する。

問 10 正解 完璧 直前チェック

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TLSで利用するディジタル証明書の規格は，ITU-T X.400で標準化されている。

イ　ディジタル証明書は，TLSプロトコルにおいて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ている。

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ディジタル署名したものである。

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

春 秋

問9　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。たとえば，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を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10　イ

解説　**ディジタル証明書**は，1988年にITUが勧告したX.509によって公開鍵証明書が標準化されている。ディジタル証明書には，シリアル番号，発行者名，有効期間，所有者名，所有者の公開鍵などの情報が含まれており，認証局の秘密鍵で電子署名が付与されている。

ア：S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-TのX.500ディレクトリシリーズのX.509で規定されている。

ウ：ディジタル証明書には，申請者の公開鍵に対して認証局の電子署名が付与されている。

エ：下位の認証局の証明書は，ルート認証局の秘密鍵で電子署名されている。

問 11 正解 完璧 直前チェック

不適合への対応のうち，JIS Q 27000:2014（情報セキュリティマネジメントシステム−用語）の“是正処置”の定義はどれか。

ア　不適合によって起こった結果に対処するための処置
イ　不適合の原因を除去し，再発を防止するための処置
ウ　不適合の性質及び対応結果について文書化するための処置
エ　不適合を除去するための処置

問 12 正解 完璧 直前チェック

JIS Q 27000:2014（情報セキュリティマネジメントシステム−用語）における情報セキュリティリスクに関する記述のうち，適切なものはどれか。

ア　脅威とは，一つ以上の要因によって悪用される可能性がある，資産又は管理策の弱点のことである。
イ　脆弱性とは，システム又は組織に損害を与える可能性がある，望ましくないインシデントの潜在的な原因のことである。
ウ　リスク対応とは，リスクの大きさが，受容可能か又は許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセスのことである。
エ　リスク特定とは，リスクを発見，認識及び記述するプロセスのことであり，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。

問11　イ

解説 **JIS Q 27000:2014**は，組織の事業リスク全般に対する考慮のもとで文書化した**ISMS**（Information Security Management System）の規格である。ISMSは，情報セキュリティマネジメントシステムと呼ばれる。組織が業務上，維持すべきセキュリティレベルを決定し，そのための計画と資源配分を策定して実際に運用することである。ISMSは外部審査機関によって審査・認証される。

是正処置は，監査で発見された不適合の原因を除去し，再発を防止するための処置である。

ア：JIS Q 27000:2014に用語の定義にはないが，改善の説明といえる。
イ：是正処置の説明である。
ウ：JIS Q 27000:2014に用語の定義にはないが，監査報告書の説明といえる。
エ：修正の説明である。

問12　エ

解説 **JIS Q 27000:2014**は，組織の事業リスク全般に対する考慮のもとで文書化した**ISMS**（Information Security Management System）の規格である。

情報セキュリティリスクは，脅威が情報資産の脆弱性または情報資産グループの脆弱性に付け込み，その結果，組織に損害を与える可能性にともなって生じるものである。

リスク対応は，リスクを修正するプロセス。リスクの回避，リスク排除，リスク予防，リスク低減を行うことである。

ア：**脆弱性**の説明である。
イ：**脅威**の説明である。
ウ：**リスク評価**の説明である。
エ：正しい。**リスク特定**の説明である。

問 13 正解 完璧 直前チェック

基本評価基準，現状評価基準，環境評価基準の三つの基準で情報システムの脆弱性の深刻度を評価するものはどれか。

ア CVSS　　イ ISMS　　ウ PCI DSS　　エ PMS

問 14 正解 完璧 直前チェック

攻撃者が，Webアプリケーションのセッションを乗っ取り，そのセッションを利用してアクセスした場合でも，個人情報の漏えいなどに被害が拡大しないようにするために，重要な情報の表示などをする画面の直前でWebアプリケーションが追加的に行う対策として，最も適切なものはどれか。

ア Webブラウザとの間の通信を暗号化する。
イ 発行済セッションIDをCookieに格納する。
ウ 発行済セッションIDをHTTPレスポンスボディ中のリンク先のURIのクエリ文字列に設定する。
エ パスワードによる利用者認証を行う。

問 15 正解 完璧 直前チェック

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

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性をもつメールサーバからの通信を遮断する。

問13　ア

解説

基本評価基準（Base Metrics）：情報システムのセキュリティの考え方である。機密性，完全性，可用性に対する影響を評価する。

現状評価基準（Temporal Metrics）：脆弱性について現在の深刻度を調査する。

環境評価基準（Environmental Metrics）：製品利用者の利用環境も含めた脆弱性について調査する。

CVSS（Common Vulnerability Scoring System）：情報システムの脆弱性に対する汎用的な評価手法である。CVSSでは，基本評価基準，現状評価基準，環境評価基準といった三つの基準で脆弱性を評価する。

ISMS（Information Security Management System）：情報セキュリティマネジメントシステム。企業が情報を適切に管理し，機密情報を守るための仕組みである。

PCI DSS（Payment Card Industry Data Security Standard）：クレジット業界の世界的なセキュリティ基準である。

PMS（Personal information protection Management Systems）：個人情報保護マネジメントシステムのことで，プライバシマーク（Pマーク）の認証取得のために必要となる管理ルールである。

問14　エ

解説 Webアプリケーションのセッションを乗っ取られ，そのセッションを利用された場合，被害者が画面上で操作できることを攻撃者が悪意をもって操作できるようになる。この場合は，利用者しか知りえない情報を追加対策として入れることが有効である。

ア：通信路を暗号化してもセッションを乗っ取られた場合は防御できない。

イ，ウ：発行済みセッションIDは，セッションを乗っ取られているためCookieへの格納や，URIのクエリ文字列へ設定しても乗っ取られてしまう。

エ：防御策として有効である。セッションを乗っ取られても，重要な情報の前でパスワードによる利用者認証が入れば，パスワードを知らない攻撃者は先へのアクセスができない。

問15　イ

解説 **OP25B**（Outbound Port 25 Blocking）は，動的IPアドレスを割り当てたネットワークから，外部ネットワークへのポート番号25の通信（SMTP）を遮断する手法である。

ウイルス感染PCや迷惑メール発信者がメールを外部サーバへ直接発信できなくするのがOP25Bである。

ア：**シグネチャマッチング方式**による対策である。

ウ：**DNSによる逆引き**を利用した対策である。

エ：**RBL**（Realtime Blackhole List）による対策である。

問 16 正解 完璧 直前チェック

外部から侵入されたサーバ及びそのサーバに接続されていた記憶媒体を調査対象としてディジタルフォレンジックスを行うことになった。まず，稼働状態にある調査対象サーバや記憶媒体などから表に示すa～dのデータを証拠として保全する。保全の順序のうち，最も適切なものはどれか。

	証拠として保全するデータ
a	遠隔にあるログサーバに記録された調査対象サーバのアクセスログ
b	調査対象サーバにインストールされていた会計ソフトのインストール用CD
c	調査対象サーバのハードディスク上の表計算ファイル
d	調査対象サーバのルーティングテーブルの状態

ア　a → c → d → b
イ　b → c → a → d
ウ　c → a → d → b
エ　d → c → a → b

問 17 正解 完璧 直前チェック

無線LANの情報セキュリティ対策に関する記述のうち，適切なものはどれか。

ア　EAPでは，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できる。
イ　RADIUSでは，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できる。
ウ　SSIDは，クライアントPCごとの秘密鍵を定めたものであり，公開鍵暗号方式による暗号化通信を実現できる。
エ　WPA2-Enterpriseでは，IEEE 802.1Xの規格に沿った利用者認証及び動的に配布される暗号化鍵を用いた暗号化通信を実現できる。

問16　エ

解説　**ディジタルフォレンジックス**は，パソコンやサーバなどのコンピュータ機器が犯罪や裁判での証拠となり得るときに，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。

設問では外部から侵入されたサーバと，サーバに接続されている記憶媒体が調査対象であるから，初めに外部からの侵入部分をチェック(d)する。その後，ファイルの改ざんチェック(c)，遠隔にあるログチェック(a)という順序になる。bのインストールCDは読み取り専用であるため，確認の優先度は最後となる。

cの後に，aとなるのは，aが遠隔にあるため，外部からの侵入では改ざんされる可能性が，cよりも低いからである。

問17　エ

解説

EAP(Extensible Authentication Protocol)：PPP(Point to Point Protocol)を拡張した認証プロトコル。ユーザID/パスワード以外にも，スマートカード(ICカード)やディジタル証明書などさまざまな認証方式をサポートしている。EAP-TLS, EAP-TTLSなどがある。

RADIUS(Remote Authentication Dial In User Service)：アクセスサーバと認証サーバ間でやり取りする認証プロトコル。クライアントが認証を求める際に，認証を必要とするサーバ(アクセスサーバ)と認証機能を分離し，利用者の一元管理，アクセスログの記録が可能となる。

SSID(Service Set ID)：無線LANのアクセスポイントを識別するためのIDである。

WPA2-Enterprise(Wi-Fi Protected Access 2 Enterprise)：WPAの改良版で，AES(Advanced Encryption Standard)を採用したCCMP(Counter-mode with CBC-MAC Protocol)暗号化方式である。WPA2は，個人の自宅のようにアクセスポイントで直接認証する。WPA2 Enterpriseは，認証サーバを利用した方式となる。

問 18 正解 完璧 直前チェック

ルータで接続された二つのセグメント間でのコリジョンの伝搬とブロードキャストフレームの中継について，適切な組合せはどれか。

	コリジョンの伝搬	ブロードキャストフレームの中継
ア	伝搬しない	中継しない
イ	伝搬しない	中継する
ウ	伝搬する	中継しない
エ	伝搬する	中継する

問 19 正解 完璧 直前チェック

1台のサーバと複数台のクライアントが，100 Mビット/秒のLANで接続されている。業務のピーク時には，クライアント1台につき1分当たり600 kバイトのデータをサーバからダウンロードする。このとき，同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台までか。ここで，LANの伝送効率は50%，サーバ及びクライアント内の処理時間は無視できるものとし，1 Mビット/秒 = 10^6ビット/秒，1 kバイト = 1,000バイトとする。

ア 10　　イ 625　　ウ 1,250　　エ 5,000

問 20 正解 完璧 直前チェック

ネットワークに接続されているホストのIPアドレスが198.51.100.90で，サブネットマスクが255.255.255.224のとき，ホストアドレスはどれか。

ア 10　　イ 26　　ウ 90　　エ 212

問18 ア

解説 ルータで接続された二つのセグメント間の通信は，OSI参照モデルで考える必要がある。コリジョンおよびブロードキャストフレームは，いずれも第2層のデータリンク層で中継される。そのため，第3層のルータでは伝搬されない。注意しなければならないのは，ブロードキャストフレームは第2層だが，ブロードキャストパケットとなると第3層になる。呼び方に注意する必要がある。

コリジョン：フレームの衝突を通知すること。

ブロードキャストフレーム：第2層で接続されている機器全体へ送付するフレーム。

OSI基本参照モデル	PDU	機器
第7層　アプリケーション層	メッセージ	ゲートウェイなど
第6層　プレゼンテーション層		
第5層　セッション層		
第4層　トランスポート層	セグメント	
第3層　ネットワーク層	パケット	ルータ，L3スイッチ
第2層　データリンク層	フレーム	ブリッジ，L2スイッチ
第1層　物理層	ビット	リピータ，ハブ

PDU（Protocol Data Unit）：各層でデータを扱う単位。

問19 イ

解説 クライアント数は，（1秒間の実効データ転送速度）÷（クライアント1台の1秒間のデータ量）で求められる。

$$(0.5 \times 100 \times 10^6 \div 8) \div (600 \times 10^3 \div 60) = (6.25 \times 10^6) \div (1 \times 10^4) = 625$$

伝送効率は，ネットワーク回線の単位時間当たりに転送できるデータ量の比率。通信量が増えると，衝突が発生して低下することがある。

問20 イ

解説 サブネットマスクから，ホストアドレスを求める。設問からサブネットマスクとホストのIPアドレスを2進数表記すると，下表のようになる。

サブネットマスク	255.	255.	255.	224
（2進数表記）	11111111.	11111111.	11111111.	11**100000**
ホストのIPアドレス	198.	51.	100.	90
（2進数表記）	11000110.	00110011.	01100100.	010**11010**

サブネットマスクの2進数表記では，下位5ビットが0となっている。ホストアドレスはこの下位5ビットで示されるところであるため，これをホストのIPアドレスの2進数表記から読み取ると，11010となる。これを10進数に変換すると，11010 = 26となる。

問 21 正解 完璧 直前チェック

ビッグデータの解析に利用されるニューラルネットワークに関する記述のうち，適切なものはどれか。

ア　誤差逆伝播法（バックプロパゲーション）は，ニューラルネットワーク全体の重みを調整する手法であり，調整作業は入力層から出力層に向かって行われる。
イ　サポートベクタマシンは機械学習に必要な機能を実現する装置のことであり，ニューラルネットワークで大量計算する際に利用される。
ウ　深層学習（ディープラーニング）に用いられるニューラルネットワークは，入力層と出力層の間に複数の中間層をもつモデルが利用される。
エ　中間層を増やしたニューラルネットワークによる訓練データを用いた学習は，訓練データ以外の未知のデータに対しても高精度な正解が導け，これを過学習（オーバフィッティング）という。

問 22 正解 完璧 直前チェック

JIS X 25010:2013（システム及びソフトウェア製品の品質要求及び評価（SQuaRE）－システム及びソフトウェア品質モデル）におけるシステムの利用時の品質特性に“満足性”がある。“満足性”の品質副特性の一つである“実用性”の説明はどれか。

ア　個人的なニーズを満たすことから利用者が感じる喜びの度合い
イ　利用者がシステム又はソフトウェアを利用するときの快適さに満足する度合い
ウ　利用者又は他の利害関係者がもつ，製品又はシステムが意図したとおりに動作するという確信の度合い
エ　利用の結果及び利用の影響を含め，利用者が把握した目標の達成状況によって得られる利用者の満足の度合い

問21　ウ

解説　**ニューラルネットワーク**は，人間の脳内にある神経細胞（ニューロン）とそのつながりといった，神経回路網を人工的にITを利用してソフトウェア的に表したものである。
ア：**誤差逆伝播法**は，出力層から入力層に向かって調整する手法である。
イ：**サポートベクタマシン**は，データの境界面を利用し分類する手法である。大量計算よりもより深く計算するものに利用される。
ウ：正しい。
エ：**オーバフィッティング**は，異常なデータ量が多すぎる場合や，必要なデータが少なすぎる場合に発生し，データの解析制度が落ちることを指す。

問22　エ

解説　**JIS X 25010:2013**は，定義された特定の条件で利用する場合の，システムの品質，システムがさまざまな利害関係者の明示的ニーズおよび暗黙のニーズを満足している度合いを表すための規格要求事項である。**満足性**は，製品又はシステムが明示された利用状況において使用されるとき，利用者ニーズが満足される度合いである。
ア：**快感性**の説明である。
イ：**快適性**の説明である。
ウ：**信用性**の説明である。
エ：正しい。**実用性**の説明である。

問 23 正解 完璧 直前チェック

企業間で，商用目的で締結されたソフトウェアの開発請負契約書に著作権の帰属が記載されていない場合，著作権の帰属先として，適切なものはどれか。

ア　請負人，注文者のどちらにも帰属しない。
イ　請負人と注文者が共有する。
ウ　請負人に帰属する。
エ　注文者に帰属する。

問 24 正解 完璧 直前チェック

情報システムの設計のうち，フェールソフトの考え方を適用した例はどれか。

ア　UPSを設置することによって，停電時に手順どおりにシステムを停止できるようにする。
イ　制御プログラムの障害時に，システムの暴走を避け，安全に運転を停止できるようにする。
ウ　ハードウェアの障害時に，パフォーマンスは低下するが，構成を縮小して運転を続けられるようにする。
エ　利用者の誤操作や誤入力を未然に防ぐことによって，システムの誤動作を防止できるようにする。

問 25 正解 完璧 直前チェック

株式会社の内部監査におけるシステム監査を，システム監査基準（平成16年）に基づいて実施する場合の監査責任者及びメンバに関する記述のうち，適切なものはどれか。

ア　あるメンバを，当該メンバが過去に在籍していた部門に対する監査に従事させる場合，一定の期間を置く。
イ　監査責任者は，当該株式会社の株主に限る。
ウ　監査部門の在籍期間について，メンバの場合は制限がないが，監査責任者の場合は会社法における監査役の任期を下回ってはならない。
エ　メンバの給与その他の報酬の水準は，監査部門に在籍中は引き下げてはならない。

春 秋

問23　ウ

解説　ソフトウェアは，注文者が依頼する仕様書に基づいて**請負人**が開発するので，著作権はソフトウェアの開発元である請負人にある。ただし，委託契約書で開発成果物の著作権の帰属先を記載してあれば，それに従う。設問では著作権の帰属先が明記されてないので請負人に著作権があり，注文者はその開発成果物を別のソフトウェアに転用できないことになる。

問24　ウ

解説　**フェールソフト**とは，システムに障害が発生した場合，障害箇所を切り離して障害の影響の拡大を防ぎ，規模を縮小して稼働を継続するシステム構成技法である。
ア：**フォールトトレランス**に関する説明である。システム障害発生時にも正常な動作を維持できるようにシステムを構成する手法。
イ：**フェールセーフ**に関する説明である。システムに故障が発生した場合，生命や周辺の機器へ損害を及ぼすことのないように，常に安全な状態にシステムを維持するシステム構成手法。
エ：**フールプルーフ**に関する説明である。利用者の誤入力や誤操作を想定し，あらかじめそのような事象が発生しないようにシステムを構成する。

問25　ア

解説　**システム監査基準**は，情報システムを適切に管理・運用することを目的とした基準である。
　具体的には以下がある。
・システム監査基準の品質を確保し，有効かつ効率的に監査を実施する。
・リスクコントロールがリスクアセスメントに基づいて整備・運用されているかをシステム監査人が評価し，保証・助言を行い，ITガバナンスの実現に寄与する。
ア：正しい。システム監査は，利害関係がないメンバが担当する必要があるため，過去に在籍していた部門に対する監査をする場合，一定期間置くのがよい。
イ：内部監査の場合，企業内の監査担当が責任者となるため，株主ではない。
ウ：内部監査の場合，会社法の監査役とは関連していない。そのため，監査責任者と，監査役の任期は関係ない。
エ：内部監査のメンバの給与の基準は，関連しない。