問題

問題文中で共通に使用される表記ルール

各問題文中に注記がない限り，次の表記ルールが適用されているものとする．

試験問題での表記	規格・標準の名称
JIS Q 9001	JIS Q 9001:2008
JIS Q 14001	JIS Q 14001:2004
JIS Q 15001	JIS Q 15001:2006
JIS Q 20000-1	JIS Q 20000-1:2012
JIS Q 20000-2	JIS Q 20000-2:2007
JIS Q 27001	JIS Q 27001:2006
JIS Q 27002	JIS Q 27002:2006
JIS X 0160	JIS X 0160:2012
ISO 21500	ISO 21500:2012
ITIL	ITIL 2011 edition
PMBOK	PMBOK ガイド 第4版
共通フレーム	共通フレーム 2013

問題

問 1

正解 完璧 直前CHECK

RLO（Right-to-Left Override）を利用した手口の説明はどれか.

ア “コンピュータウイルスに感染している”といった偽の警告を出して利用者を脅し，ウイルス対策ソフトの購入などを迫る.

イ 脆弱性があるホストやシステムをあえて公開し，攻撃の内容を観察する.

ウ ネットワーク機器のMIB情報のうち監視項目の値の変化を感知し，セキュリティに関するイベントをSNMPマネージャに通知するように動作させる.

エ 文字の表示順を変える制御文字を利用し，ファイル名の拡張子を偽装する.

問 2

正解 完璧 直前CHECK

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 エンベローピング署名（Enveloping Signature）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 3

正解 完璧 直前CHECK

共通鍵暗号方式で，100人の送受信者のそれぞれが，相互に暗号化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1　エ

RLO（Right-to-Left Override）：Unicodeで定義されている制御文字の流れを，右から左に変更することで，ウイルスがファイル名の拡張子を偽造する．

ア：「偽セキュリティ対策ソフト型」ウイルスの説明である．

イ：ハニーポットの説明である．

問2　ア

XMLディジタル署名はXML文書に付ける署名である．署名アルゴリズムや，証明書や署名のタグを定め，任意のデータに署名を付けられるだけでなく，XML文書の指定したエレメントやコンテントに対して署名を付けることもできる．

イ：署名要素が署名対象要素の子要素となる署名形式であるため，同じ文書に複数人の署名を付けるなどの用途に適しているが，必ず複数の署名を付ける訳ではない．

ウ：署名形式はXML（XML-Signature Syntax and Processing）である．CMSはASN.1で規定されており，S/MIMEやPKI用途で利用されている．

エ：署名対象，署名アルゴリズムや署名値および証明書などをXMLの文法で記述する．ASN.1構文に比べてXMLディジタル署名は，XMLタグ付き言語であるためわかりやすい．

問3　イ

ある一人から見ると通信相手は99人なので，共通鍵も99個必要となる．100人では99×100 = 9,900個が必要となるが，同じ相手とは同じ共通鍵を送受信で使うので，半分（9,900/2 = 4,950）となる．

問 4

正解 完璧 直前CHECK

無線LANにおけるWPA2の特徴はどれか.

ア　AHとESPの機能によって認証と暗号化を実現する.
イ　暗号化アルゴリズムにAESを採用したCCMP（Counter-mode with CBC-MAC Protocol）を使用する.
ウ　端末とアクセスポイントの間で通信を行う際に，SSL Handshake Protocolを使用して，お互いが正当な相手かどうかを認証する.
エ　利用者が設定する秘密鍵と，製品で生成するIV（Initialization Vector）とを連結した数字を基に，データをフレームごとにRC4で暗号化する.

問 5

正解 完璧 直前CHECK

JVN（Japan Vulnerability Notes）などの脆弱性対策ポータルサイトで採用されているCVE（Common Vulnerabilities and Exposures）識別子の説明はどれか.

ア　コンピュータで必要なセキュリティ設定項目を識別するための識別子である.
イ　脆弱性を利用して改ざんされたwebサイトの画面ショットを識別するための識別子である.
ウ　製品に含まれる脆弱性を識別するための識別子である.
エ　セキュリティ製品を識別するための識別子である.

問 6

正解 完璧 直前CHECK

サイドチャネル攻撃の手法であるタイミング攻撃の対策として，最も適切なものはどれか.

ア　演算アルゴリズムに対策を施して，機密情報の違いによって演算の処理時間に差異が出ないようにする.
イ　故障を検出する機構を設けて，検出したら機密情報を破壊する.
ウ　コンデンサを挿入して，電力消費量が時間的に均一になるようにする.
エ　保護層を備えて，内部のデータが不正に書き換えられないようにする.

問4　イ

WPA2（Wi-Fi Protected Access 2）：WPAの改良版で，AES（Advanced Encryption Standard）を採用したCCMP（Counter-mode with CBC-MAC Protocol）暗号化方式を採用している．無線の暗号化は，WEPがセキュリティ的に脆弱だということでWPAが作られ，さらに強力なWPA2が作られた．日々の技術進歩により，暗号を解読できる速度が速くなるためより強力な暗号技術が必要となっている．

WPA（Wi-Fi Protected Access）：WEPで存在したセキュリティ面での脆弱点を補強し強化したもの．

AES（Advanced Encryption Standard）：共通かぎ暗号方式のブロック暗号であり，DESの後継規格となった米国政府標準暗号である．かぎ長は128ビット，192ビット，256ビットの3種から選択できる．

ア：IPsec（IP Security Protocol）の説明である．

エ：WEP（Wired Equivalent Privacy）の説明である

問5　ウ

JVN（Japan Vulnerability Notes）は，日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し，情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトである．JPCERTコーディネーションセンター（JPCERT/CC）と，独立行政法人情報処理推進機構（IPA）が共同運営している．

CVEは，脆弱性を識別するための識別子である．

問6　ア

サイドチャネル攻撃は，暗号を解読するための攻撃手法の一つである．暗号化や復号の際に発生する電磁波，熱，演算処理時間など暗号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．

ア：**タイミング攻撃対策**の説明である．

イ：**故障利用攻撃対策**の説明である．

ウ：**電力解析攻撃対策**の説明である．

問題

問 7

正解 □ 完璧 □ 直前CHECK □

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　ディスプレイなどから放射される電磁波を傍受し、表示内容などを盗み見る技術であり，電磁波を遮断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，ディジタル署名を利用した改ざん検知によって対抗する．

ウ　マクロウイルスにおい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の信号を傍受し，通信内容を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 8

正解 □ 完璧 □ 直前CHECK □

DMZ上のコンピュータがインターネットからのpingに応答しないようにファイアウォールのルールを定めるとき，“通過禁止”に設定するものはどれか．

ア　ICMP

イ　TCP及びUDPのポート番号53

ウ　TCPのポート番号21

エ　UDPのポート番号123

問 9

正解 □ 完璧 □ 直前CHECK □

共通鍵暗号の鍵を見つけ出す，ブルートフォース攻撃に該当するものはどれか．

ア　1組の平文と暗号文が与えられたとき，全ての鍵候補を一つずつ試して鍵を見つけ出す．

イ　平文と暗号文と鍵の関係を代数式に表して数学的に鍵を見つけ出す．

ウ　平文の一部分の情報と暗号文の一部分の情報との間の統計的相関を手掛かりに鍵を見つけ出す．

エ　平文を一定量変化させたときの暗号文の変化から鍵を見つけ出す．

問7　ア

テンペスト技術とは，電子機器やケーブルから漏えいする電磁波に関するセキュリティ上の対策のことである．具体的には，回路設計の段階で信号の漏えいを防ぎつつ，ケーブル等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，パソコン等が入った部屋全体をシールドするという手段もある．

イ：データの改ざん対策の説明である．

ウ：ウイルス対策の説明である．

エ：無線LANの盗聴対策の説明である．

問8　ア

pingは**ICMP**（Internet Control Message Protocol）を使用するので，ICMPを通過禁止にする．pingを利用することで，DMZ上のサーバの有無を攻撃者に知らせることになるため，一般的には禁止が良いとされる．

イ：TCPとUDPのポート番号53はDNSに使用される．

ウ：TCPポート番号21はFTP（制御）に使用される．FTPを禁止にする場合には，FTP（データ）のTCPポート番号20も通過禁止にする．

エ：UDPポート番号123はNTPに使用される．

問9　ア

ブルートフォース攻撃は総当たり攻撃とも呼ばれ，考えられるすべてのかぎをリストアップして解読を試みる方式である．どのような暗号方式に対しても攻撃できるが，鍵長が長くなると考えられる鍵のパターンの数が幾何級数的に増大するため，効率の悪い攻撃方法といえる．

イ：**線形攻撃**の説明である．

エ：**差分攻撃**の説明である．

問題

問 10

正解 完璧 直前CHECK

利用者PCがボットに感染しているかどうかをhostsファイルで確認するとき，設定内容が改ざんされていないと判断できるものはどれか．ここで，hostsファイルには設定内容が1行だけ書かれているものとする．

	設定内容	説　明
ア	127.0.0.1　a.b.com	a.b.comはOS提供元のFQDNを示す.
イ	127.0.0.1　c.d.com	c.d.comはPC製造元のFQDNを示す.
ウ	127.0.0.1　e.f.com	e.f.comはウイルス定義ファイルの提供元のFQDNを示す.
エ	127.0.0.1　localhost	localhostは利用者PC自身を示す.

問 11

正解 完璧 直前CHECK

ルートキット（rootkit）を説明したものはどれか.

ア　OSの中核であるカーネル部分の脆弱(ぜい)性を分析するツール
イ　コンピュータがウイルスやワームに感染していないことをチェックするツール
ウ　コンピュータやルータのアクセス可能な通信ポートを外部から調査するツール
エ　不正侵入してOSなどに組み込んだものを隠蔽するツール

問 12

正解 完璧 直前CHECK

送信元を詐称した電子メールを拒否するために，SPF（Sender Policy Framework）の仕組みにおいて受信側が行うことはどれか.

ア　Resent-Sender:，Resent-From:，Sender:，From:などのメールヘッダの送信者メールアドレスを基に送信メールアカウントを検証する.
イ　SMTPが利用するポート番号25の通信を拒否する.
ウ　SMTP通信中にやり取りされるMAIL FROMコマンドで与えられた送信ドメインと送信サーバのIPアドレスの適合性を検証する.
エ　電子メールに付加されたディジタル署名を検証する.

問10　エ

ボットは，コンピュータウイルスの一種で，PCを外部から操ることを目的として作成されたプログラムである．ボットに感染すると，自分のPCから迷惑メールを発信されることや，DoS攻撃の踏み台になることがある．

127.0.0.1は，自分のホストを示すIPアドレスであるため，localhost以外が指定されている場合は不正である．

問11　エ

ルートキットとは，**クラッカ**が**セキュリティホール**等を利用して不正侵入した後に，侵入の隠ぺい，バックドアの確保，踏み台による攻撃等に用いる機能をまとめたツール群のことである．

イ：ウイルス対策ソフトの説明である．

ウ：ポートスキャンツールの説明である．

問12　ウ

SPF（Sender Policy Framework）：差出人のメールアドレスが他のドメインになりすましていないかどうかを検出する，電子メールにおける送信ドメイン認証の仕組み．

ア：**スパムメール**は実在しないドメインのメールアカウントを使用することが多いことから，スパムメールの判定に利用されることがある．メールヘッダ情報の送信者メールアドレスが実在するメールアカウントに詐称されているとチェックできない．

イ：**OP25B**（Outbound Port 25 Blocking）の説明である．外部のSMTPサーバへの通信を遮断することでスパムメールの送信やウイルスの拡散を防ぐ．主にISPで行われる．

エ：**DKIM**（Domain Keys Identified Mail）の説明である．送信元メールサーバがメールに付加したディジタル署名を受信側がチェックすることで，送信元の正当性を確認する．

問 13

正解 □ 完璧 □ 直前CHECK □

迷惑メールの検知手法であるベイジアンフィルタリングの説明はどれか.

ア　信頼できるメール送信元を許可リストに登録しておき，許可リストにないメール送信元からの電子メールは迷惑メールと判定する.

イ　電子メールが正規のメールサーバから送信されていることを検証し，迷惑メールであるかどうかを判定する.

ウ　電子メールの第三者中継を許可しているメールサーバを登録したデータベースに掲載されている情報を基に，迷惑メールであるかどうかを判定する.

エ　利用者が振り分けた迷惑メールから特徴を学習し，迷惑メールであるかどうかを統計的に解析して判定する.

問 14

正解 □ 完璧 □ 直前CHECK □

DNSの再帰的な問合せを使ったサービス不能攻撃（DNS amp）の踏み台にされるとこを防止する対策はどれか.

ア　キャッシュサーバとコンテンツサーバに分離し，インターネット側からキャッシュサーバに問合せできないようにする.

イ　問合せがあったドメインに関する情報をWhoisデータベースで確認する.

ウ　一つのDNSレコードに複数のサーバのIPアドレスを割り当て，サーバへのアクセスを振り分けて分散させるように設定する.

エ　他の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ディジタル署名で確認するように設定する.

問 15

正解 □ 完璧 □ 直前CHECK □

SQLインジェクション対策について，Webアプリケーションの実装における対策とWebアプリケーションの実装以外の対策として，ともに適切なものはどれか.

	Webアプリケーションの実装における対策	Webアプリケーションの実装以外の対策
ア	Webアプリケーション中でシェルを起動しない.	chroot環境でWebサーバを実行する.
イ	セッションIDを乱数で生成する.	SSLによって通信内容を秘匿する.
ウ	バインド機構を利用する.	データベースのアカウントのもつデータベースアクセス権限を必要最小限にする.
エ	パス名やファイル名をパラメタとして受け取らないようにする.	重要なファイルを公開領域に置かない.

問13　エ

ベイジアンフィルタリングは，ベイズ理論を用いた自己学習型スパムメールフィルタである．スパムの要素を示す言葉と特徴のリストを自動生成し，フィルタリングする仕組みである．

ベイズ理論とは，過去の事象の発生確率から統計的に解析して予測する理論である．提唱者であるトーマス・ベイズ（Thomas Bayes）の名前がつけられている，

ア：メールサーバの**アクセスリスト**による対策の説明である．

イ：**送信ドメイン認証**による対策の説明である．

ウ：**ブラックリスト**を利用した対策の説明である．

エ：**ベイジアンフィルタリング**の説明である．自己学習し統計的に解析する点に注目するのが良い．

問14　ア

DNSの再帰的な問い合わせを使ったサービス不能攻撃（**DNS amp**）は**DDoS**（Distributed Denial of Service）の一種である．DNSキャッシュサーバを踏み台とし，送信元を偽装したDNSクエリによりDNSサーバを攻撃する手法である．

対策は，**DNSキャッシュポイズニング**の脆弱性対策を行うことや，通常一つになっているキャッシュサーバの機能とコンテンツサーバの機能を分離して，コンテンツサーバを守ることである．

DNSキャッシュサーバ：DNSの参照に必要な一時的なデータのみを保管する．

DNSコンテンツサーバ：DNSのゾーン情報を持ち，恒久的なデータを保管する．

ア：正しい．DNS ampはキャッシュサーバを狙って攻撃をする．

イ：**Whois**でドメイン情報を検索しても踏み台の防止にはならない．Whoisは，IPアドレスやドメイン名の登録者に関する情報を検索，提供可能とするサービスである．

ウ：**DNSラウンドロビン**の説明である．

問15　ウ

SQLインジェクションは，アプリケーションの想定しないSQL文を実行することでデータベースシステムを不正に操作し，データの取得や書き換えなどを可能とする攻撃のことである．対策としては，**バインド機構**や**エスケープ処理**を用いる．

バインド機構は，SQL文のひな型を用意し，後から可変値の部分に入力値を割り当ててSQL文を生成する．

エスケープ処理は，特殊な意味を持つ文字列をチェックして特殊文字を置き換える．また，データベースのアカウントの持つアクセス権を必要最小限にして，最低限な機能のみを実行可能としておくことも必要である．

問題

問 16

正解 完璧 直前CHECK

ディレクトリトラバーサル攻撃はどれか.

ア　攻撃者が，OSの操作コマンドを利用するアプリケーションに対して，OSのディレクトリ作成コマンドを渡して実行する.

イ　攻撃者が，SQL文のリテラル部分の生成処理に問題があるアプリケーションに対して，任意のSQL文を渡して実行する.

ウ　攻撃者が，シングルサインオンを提供するディレクトリサービスに対して，不正に入手した認証情報を用いてログインし，複数のアプリケーションを不正使用する.

エ　攻撃者が，ファイル名の入力を伴うアプリケーションに対して，上位のディレクトリを意味する文字列を使って，非公開のファイルにアクセスする.

問 17

正解 完璧 直前CHECK

LANの制御方式に関する記述のうち，適切なものはどれか.

ア　CSMA/CD方式では，単位時間当たりの送出フレーム数が増していくと，衝突の頻度が増すので，スループットはある値をピークとして，その後下がる.

イ　CSMA/CD方式では，一つの装置から送出されたフレームが順番に各装置に伝送されるので，リング状のLANに適している.

ウ　TDMA方式では，伝送路上におけるフレームの伝搬遅延時間による衝突が発生する.

エ　トークンパッシング方式では，トークンの巡回によって送信権を管理しているので，トラフィックが増大すると，CSMA/CD方式に比べて伝送効率が急激に低下する.

問 18

正解 完璧 直前CHECK

コンピュータとスイッチングハブ（レイヤ2スイッチ）の間，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16　エ

ディレクトリトラバーサル攻撃とは，相対パス記法を利用して，管理者や利用者の想定とは別のディレクトリのファイルを指定するソフトウェアの攻撃方法である．相対パス記法を悪用したディレクトリトラバーサル攻撃を受けた場合，許可されたディレクトリ・ファイル以外の意図しないファイルが読み出され，情報が漏えいすることや，既存のファイルが破壊されるなどの危険がある．

問17　ア

CSMA/CDでは，伝送路上にフレームがなければどのノードでもデータを送出できる．複数のノードが同時にデータを送出する可能性もあり，この場合は衝突が発生する．衝突した場合は，時間をおいて再度データを送出する．送出フレーム数が増大すると，この再度送出したフレームがまた衝突する危険性を持つ．したがって，送出フレーム数が増大しすぎるとスループットの低下を招くことになる．

イ：CSMA/CDではなく**トークンリングの伝送**のことである．

ウ：**TDMA**（Time Division Multiple Access）では，時間で分割されたスロットを用いる．伝搬遅延時間による衝突を防ぐため，スロットとスロットの間にガードタイムが設けられている．

エ：**トークンパッシング**はトークンを持つものだけがアクセスできるので，トラフィックが増大しても伝送効率の低下は生じにくい．

問18　エ

スパニングツリー：リング型のネットワークでデータが永久に循環するのを防ぐための方式の一つ．

ブリッジ：データリンク層でデータを中継するための装置．

マルチホーミング：複数の経路を選択して同時に使用することで，負荷を分散することが可能となる．論理的に1本の回線として扱っているわけではない．

リンクアグリゲーション：複数の物理回線を論理的に1本に束ねて高速の回線として利用する．

問題

問 19

正解 完璧 直前CHECK

電子メールシステムにおいて，利用者端末がサーバから電子メールを受信するために使用するプロトコルであり，選択した電子メールだけを利用者端末へ転送する機能，サーバ上の電子メールを検索する機能，電子メールのヘッダだけを取り出す機能などをもつものはどれか．

ア　IMAP4　　イ　MIME　　ウ　POP3　　エ　SMTP

問 20

正解 完璧 直前CHECK

TCPのサブミッションポート（ポート番号587）の説明として，適切なものはどれか．

ア　FTPサービスで，制御用コネクションのポート番号21とは別にデータ転送用に使用する．

イ　Webアプリケーションで，ポート80番のHTTP要求とは別に，サブミットボタンをクリックした際の入力フォームのデータ送信に使用する．

ウ　コマンド操作の遠隔ログインで，通信内容を暗号化するためにTELNETのポート番号23の代わりに使用する．

エ　電子メールサービスで，迷惑メール対策としてSMTPのポート番号25の代わりに使用する．

問 21

正解 完璧 直前CHECK

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，利用者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，利用者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，利用者はそれを意識せずに利用できること

エ　利用者がデータベースの位置を意識せずに利用できること

問19　ア

IMAP4（Internet Message Access Protocol）：受信したメールへのアクセス用プロトコルである．メールデータはサーバに残すのが特徴．

MIME（Multipurpose Internet Mail Extensions）：電子メールでテキスト以外の画像等を送付可能とするため拡張仕様である．

POP3（Post Office Protocol 3）：受信したメールへのアクセス用プロトコルである．POP3はメールサーバからクライアントPCにメールデータを全てダウンロードし，クライアントPC側にメールを蓄積する．

SMTP（Simple Mail Transfer Protocol）：電子メールの送受信用プロトコルである．サーバ対サーバ間のメールの通信に利用される．

問20　エ

TCPのサブミッションポートは，587番ポートを利用したメール送信専用ポートのことである．従来利用されてきたSMTPのポート25番の代わりに使用する．SMTPの25番ポートはスパムメールで利用されるといったセキュリティ上のリスクが高くなってきている．そのためメールを送信するプロバイダは，サブミッションポートを利用し，認証技術などを組み合わせてメール送信を行い，スパムメールの送信を回避している．

問21　ウ

分散データベースの透過性とは，データベースが複数に分散していても利用者が意識せずに利用可能となることである．

ア：移動に対する透過性に関する記述である．

イ：複製に対する透過性に関する記述である．

ウ：分割に対する透過性に関する記述である．

エ：資源位置に対する透過性に関する記述である．

問題

問 22

正解 完璧 直前CHECK

安全性と信頼性について，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，その前提条件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 23

正解 完璧 直前CHECK

表は，システムへの要求の明確さに応じた開発方針と，開発方針に適した開発モデルの組である．a ～ cに該当する開発モデルの組合せはどれか．

要求の明確さ	開発方針	開発モデル
要求が明確になっている．	全機能を一斉に開発する．	a
要求に不明確な部分がある．	簡易なシステムを実装し，動作を評価しながら要求を早期に明確にする．その後は全機能を一斉に開発する．	b
要求に変更される可能性が高い部分がある．	最初に要求が確定した部分だけを開発する．その後に要求が確定した部分を逐次追加していく．	c

	a	b	c
ア	ウォータフォールモデル	進化的モデル	プロトタイピングモデル
イ	ウォータフォールモデル	プロトタイピングモデル	進化的モデル
ウ	進化的モデル	ウォータフォールモデル	プロトタイピングモデル
エ	プロトタイピングモデル	ウォータフォールモデル	進化的モデル

問 22　ア

人が誤りを犯しても，問題が発生しないようにあらかじめ対策しておく考え方を**フールプルーフ**と呼ぶ．入力データのチェック機能を組み込むことはフールプルーフに相当する．

イ：故障の発生時に，障害を及ぼさない安全な状態になるように設計すること．踏み切りを例とすると，踏み切りの故障の場合は遮断機を自動的に下ろし，事故を未然に防ぐ方向に動作することである．

ウ：障害の発生時に，故障箇所を切り離すなどで，最低限のシステム稼働を続けること．

エ：装置の二重化などで，障害が発生しても，システムに影響を与えないようにすること

問 23　イ

ウォータフォール型手法：システム全体を一括して管理し，分析・設計・実装・テスト・運用の順に上流工程から下流工程へ開発を進める手法．各工程が完了する際に，前の工程への後戻りが起こらないよう，綿密なチェックを行う．水が滝を流れ落ちるように開発が進んでいくことから「ウォータフォール」と名付けられた．

プロトタイピング：試作品を作り，ユーザに評価してもらうことで相互の認識の違いに起因するシステム開発の失敗を回避する開発手法．要求に不明確な点がある場合は，試作品を見ることで要求内容を明確にしていくことができる．

進化的モデル：要求内容が変更されることがある場合，最初に明確化した要求部分から順次開発していく．

問題

問 24

正解 □ 完璧 □ 直前CHECK □

ITサービスマネジメントの問題管理プロセスにおけるプロアクティブな活動はどれか.

ア　インシデントの根本原因を究明する.
イ　過去に同様のインシデントが発生していないか調査する.
ウ　過去のインシデントの記録を分析し，今後起こりそうなインシデントを予測する.
エ　根本原因を突き止めた問題を既知のエラーとして登録する.

問 25

正解 □ 完璧 □ 直前CHECK □

被監査企業がSaaSをサービス利用契約して業務を実施している場合，被監査企業のシステム監査人がSaaSの利用者環境からSaaSへのアクセスコントロールを評価できる対象のIDはどれか.

ア　DBMSの管理者ID
イ　アプリケーションの利用者ID
ウ　サーバのOSの利用者ID
エ　ストレージデバイスの管理者ID

問24　ウ

プロアクティブな活動とは，問題が発生する前に，問題が起こらないようにするための活動である．問題管理では，プロアクティブな活動（防火，予防）と，リアクティブな活動（火消し，対処）がある．

ア，イ，エ：全て発生後の対応であるため，リアクティブな活動である．

問25　イ

SaaS（Software as a Service）では，ユーザが必要とするソフトウェアの機能のみを提供する仕組みで，複数利用者がマルチテナントで利用している．設問には，「SaaSの利用者環境からSaaSへのアクセスコントロールを評価できる対象のID」とあるため，SaaSで提供されるソフトウェアへのアクセス権のみが対象となる．事業主自身が利用するIDは，SaaS利用者へ提供されていないため設問の対象外といえる．

ア，ウ，エ：SaaS提供者が管理するIDである．