問題

問 1

正解 □ 完璧 □ 直前CHECK □

クリックジャッキング攻撃に該当するものはどれか.

ア　Webアプリケーションの脆弱性を悪用し，Webサーバに不正なリクエストを送ってWebサーバからのレスポンスを二つに分割させることによって，利用者のブラウザのキャッシュを偽造する.

イ　Webページのコンテンツ上に透明化した標的サイトのコンテンツを配置し，利用者が気づかないうちに標的サイト上で不正操作を実行させる.

ウ　ブラウザのタブ表示機能を利用し，ブラウザの非活性なタブの中身を，利用者が気づかないうちに偽ログインページに書き換えて，それを操作させる.

エ　利用者のブラウザの設定を変更することによって，利用者のWebページの閲覧履歴やパスワードなどの機密情報を盗み出す.

問 2

正解 □ 完璧 □ 直前CHECK □

作成者によってディジタル署名された電子文書に，タイムスタンプ機関がタイムスタンプを付与した．この電子文書を公開する場合のタイムスタンプの効果のうち，適切なものはどれか.

ア　タイムスタンプを付与した時刻以降に，作成者が電子文書の内容を他の電子文書へコピーして流用することを防止する.

イ　タイムスタンプを付与した時刻以降に，第三者が電子文書の内容を他の電子文書へコピーして流用することを防止する.

ウ　電子文書がタイムスタンプの時刻以前に存在したことを示すことによって，作成者が電子文書の作成を否認することを防止する.

エ　電子文書がタイムスタンプの時刻以前に存在したことを示すことによって，第三者が電子文書を改ざんすることを防止する.

問1　イ

クリックジャッキング攻撃：Webページのコンテンツ上に透明化した不正コンテンツを配置し，あたかも正しいサイトを操作しているように見えるが実際は不正コンテンツ上で操作をわせるようWebページを偽装することである．PCのマウスクリックを乗っ取る（jack）攻撃である．

2009年にJPCERTからクリックジャッキングに関する技術メモが公開され，その中で対策や注意喚起が行われている．

ア：**HTTPレスポンス分割攻撃**（HTTP Response Splitting Attack）の説明である．

ウ：**タブナビング**（Tabnabbing）の説明である．

エ：**ブラウザハイジャッカー**（Browser Hijacker）の説明である．

問2　ウ

タイムスタンプ：単にタイムスタンプといった場合，ファイルなどの電子データにおいて，その作成や更新などが行われた日時を示す情報を意味する．タイムスタンプ機関によるタイムスタンプは，電子データに対して正確な日付情報を付与し，その時点での電子データの存在証明と非改ざん証明を行う仕組みあるいは技術を意味する．タイムスタンプは電子公証，電子署名法において利用され，知的財産やプレスリリースといった新規性の証明や発行日時の証明が必要な電子文書に付与する．タイムスタンプ技術の国際標準としは，IETF RFC 3161（Time Stamp Protocol）という規格がある．

ア，イ：タイムスタンプでは文書のコピーを防止することはできない．

エ：改ざんすることは防止できない．タイムスタンプによる効果は改ざんされていないことの証明である．

問 3

正解 □ 完璧 □ 直前CHECK □

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で規定されている．

イ　ディジタル証明書は，SSL/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，下位層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．

問 4

正解 □ 完璧 □ 直前CHECK □

米国NISTが制定した，AESにおける鍵長の条件はどれか．

ア　128ビット，192ビット，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ビット長くする．

エ　暗号化処理単位のブロック長より32ビット短くする．

問 5

正解 □ 完璧 □ 直前CHECK □

コンティンジェンシープランにおける留意点はどれか．

ア　企業の全てのシステムを対象とするのではなく，システムの復旧の重要性と緊急性を勘案して対象を決定する．

イ　災害などへの対応のために，すぐに使用できるよう，バックアップデータをコンピュータ室内又はセンタ内に保存しておく．

ウ　バックアップの対象は，機密情報の中から機密度を勘案して選択する．

エ　被害のシナリオを作成し，これに基づく“予防策策定手順”を策定する．

問3　イ

ディジタル証明書は，ITU-Tで公開鍵証明書の標準として**X.509**が策定され，そのX.509v3をもとにインターネット利用を目的とした公開鍵証明書がIETFでRFCとして標準化された．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，所有者の公開鍵等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，申請者の公開鍵に認証局の電子署名が付与されている．

エ：下位認証局の証明書は，ルート認証局の秘密鍵で電子署名されている．

問4　ア

米国NIST（National Institute of Standards and Technology）は，米国国立標準技術研究所の略で，工業技術の標準化を支援する機関である．**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ビットを選択可能な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5　ア

ア：**コンティンジェンシープラン**（緊急時対応計画，非常事態対応計画）では企業内の全システムを復旧させる必要はない．重要度（緊急事態発生時予想損害額），対応コストを考慮して対象を選択し，有効性の高い対策を検討する．

イ：リスク分散の観点から，バックアップは別の場所保管が望ましい．

ウ：重要情報（紛失したら困る情報）と機密情報（漏れたら困る情報）は，必ずしも一致しない．

エ：予防策策定手順の立案は緊急事態発生前の平常時運用手順であり，コンティンジェンシープランではない．

問 6

正解 □ 完璧 □ 直前CHECK □

JIS Q 27001:2006における情報システムのリスクとその評価に関する記述のうち，適切なものはどれか．

ア　脅威とは，脆弱(ぜい)性が顕在化する源のことであり，情報システムに組み込まれた技術的管理策によって脅威のレベルと発生の可能性が決まる．

イ　脆弱性とは，情報システムに対して悪い影響を与える要因のことであり，自然災害，システム障害，人為的過失及び不正行為に大別される．

ウ　リスクの特定では，脅威が管理策の脆弱性に付け込むことによって情報資産に与える影響を特定する．

エ　リスク評価では，リスク回避とリスク低減の二つに評価を分類し，リスクの大きさを判断して対策を決める．

問 7

正解 □ 完璧 □ 直前CHECK □

ファイアウォールにおいて，自ネットワークのホストへの侵入を防止する対策のうち，IPスプーフィング（spoofing）攻撃の対策について述べたものはどれか．

ア　外部から入るTCPコネクション確立要求パケットのうち，外部へのインターネットサービスの提供に必要なもの以外を破棄する．

イ　外部から入るUDPパケットのうち，外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を破棄する．

ウ　外部から入るパケットの宛先IPアドレスが，インターネットとの直接の通信をすべきでない自ネットワークのホストのものであれば，そのパケットを破棄する．

エ　外部から入るパケットの送信元IPアドレスが自ネットワークのものであれば，そのパケットを破棄する．

問6　ウ

JIS Q 27001:2006：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）の確立，導入，運用，監視，レビュー，維持及び改善のための要求事項が規定されている．

ア：**脅威**とは，システムまたは組織に損害を与える可能性があるインシデントとの潜在的な原因である．

イ：**脆弱性**とは，一つ以上の脅威が付け込むことのできる資産または資産グループが持つ弱点である．

エ：**リスク対応**の選択肢については，リスクの回避，リスクの最適化，リスクの移転，リスクの保有の四つがある．

問7　エ

IPスプーフィングとは，攻撃者が送信元を隠ぺいするために，送信元IPアドレスを偽装したパケットを相手に送りつけることである．外部からのパケットは，通常であれば発信元「外部」，あて先「自ネットワーク」となる．

選択肢エでは，外部から送られてくるにもかかわらず，発信元が自ネットワークとしたパケットを破棄しているためIPスプーフィングの対策となる．

ア，イ，ウ：不正アクセスに対する防止策である．

問題

問 8

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，演算内容による処理時間の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となるようにする．
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 9

正解 完璧 直前CHECK

PCIデータセキュリティ基準（PCI DSS Version 2.0）の要件のうち，詳細要件の選択肢として，WAFの導入を含むものはどれか．

ア　要件1：カード会員データを保護するために，ファイアウォールをインストールして構成を維持すること
イ　要件3：保存されるカード会員データを保護すること
ウ　要件6：安全性の高いシステムとアプリケーションを開発し，保守すること
エ　要件7：カード会員データへのアクセスを，業務上必要な範囲内に制限すること

問8　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．

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9　ウ

PCI（Payment Card Industry）データセキュリティ基準は，クレジットカードのカード会員のデータセキュリティを強化し，均一なデータセキュリティ評価基準を推進するために策定されたものである．詳細要件は12個の定義からなる．

要件1	カード会員データを保護するために，ファイアーウォールをインストールして構成を維持する
要件2	システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
要件3	保護されるカード会員データの保護
要件4	オープンな公共ネットワーク経由でカード会員データを伝播する場合，暗号化する
要件5	アンチウィルスソフトウェアまたはプログラムを使用し，定期的に更新する
要件6	安全性の高いシステムとアプリケーションを開発し，保持する
要件7	カード会員データへのアクセスを，業務上必要な範囲内に制限する
要件8	コンピュータにアクセスできる各ユーザに一意のIDを割り当てる
要件9	カード会員データの物理アクセスを制限する
要件10	ネットワークリソースおよびカード会員データの全てのアクセスを追跡および監視する
要件11	セキュリティシステムおよびプロセスを定期的にテストする
要件12	全ての担当者の情報セキュリティポリシーを整備する

要件6.6に「アプリケーションの手前に，Webアプリケーションファイアウォール（WAF）をインストールする．」項目があるため，ウが正解となる．

表に示される全ての要件と対策を覚えるのは困難であるため，各要件で定義される範囲を覚え，消去法により選択肢を狭めて解答する．また，インターネットでPCIデータセキュリティ基準Version 2.0 を検索して，理解を深めると良い．

問 10

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セキュリティ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 11

正解 □ 完璧 □ 直前CHECK □

有料の公衆無線LANサービスにおいて実施される，ネットワークサービスの不正利用に対するセキュリティ対策の方法と目的はどれか．

ア　利用者ごとに異なるSSIDを割り当てることによって，利用者PCへの不正アクセスを防止する．
イ　利用者ごとに異なるサプリカントを割り当てることによって，利用者PCへの不正アクセスを防止する．
ウ　利用者ごとに異なるプライベートIPアドレスを割り当てることによって，第三者によるアクセスポイントへのなりすましを防止する．
エ　利用者ごとに異なる利用者IDを割り当て，パスワードを設定することによって，契約者以外の利用者によるアクセスを防止する．

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情報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受信側が検証する．

問10　ア

pingは**ICMP**（Internet Control Message Protocol）を使用するので，ICMPを通過禁止にする．

イ：TCPとUDPのポート番号53はDNSで使用される．

ウ：TCPポート番号21はFTP（File Transfer Protocol）の制御用に使用される．FTPを禁止する場合には，FTPのデータ用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（Network News Transfer Protocol）に使用される．

問11　エ

有料の**公衆無線LAN**は，利用料金を支払うことで誰でも利用可能となるサービスである．そのため，セキュリティ対策は，不特定多数が利用することや，サービスとして実現性のある技術，運用を考慮して行う必要がある．

ア：**SSID**を利用者単位に割り振った場合，SSIDは外部からも参照可能ため，セキュリティ対策の対応としては不十分である．また，SSIDの設定可能な個数制限等は技術的にも不可能である．

イ：**サプリカント**（認証用の機器やソフトウェア）は，個人用に作成すると膨大なコストがかかるため，現実的ではない．

ウ：**プライベートIDアドレス**は，範囲の限られているIPアドレスから推測したり，一つのIPアドレスを聞いたりすることで，そこから他の利用者を推測できる．

エ：利用者ごとにID，パスワードを設定する方法は，個人のみが知りえるパスワードで認証が可能であるため，不特定多数利用の場合は有効である．

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．

問題

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　迷惑メールを利用者が振り分けるときに，迷惑メールの特徴を自己学習し，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）の踏み台にされること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　問合せされ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．

問題

問 15

正解 □ 完璧 □ 直前CHECK □

SMTP-AUTHを使ったメールセキュリテイ対策はどれか.

ア　ISP管理下の動的IPアドレスからの電子メール送信について，管理外ネットワークのメールサーバへのSMTP通信を禁止する.

イ　PCからの電子メール送信は，POP接続で利用者認証済の場合にだけ許可する.

ウ　通常のSMTPのポートとは別のサブミッションポートを使用して，PCからメールサーバへの電子メール送信時の認証を行う.

エ　電子メール送信元のサーバについてDNSの逆引きが成功した場合にだけ，電子メール受信を許可する.

問 16

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を複雑なものにする.	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15　ウ

SMTP-AUTHは，クライアントがメールを送る際，SMTPサーバへのアクセス時にユーザ認証を行い，認証されたクライアントのみに電子メールの送信を許可する方式である．

ア：電子メール広告企業やウイルス感染してボット化したPCなどからのメール発信を阻止するために，管理外のメールサーバへSMTP通信の利用を防止する対策．**OP25B**（Outbound Port 25 Blocking）という．

イ：**POP before SMTP**の説明．電子メールの送信を行う際のユーザ認証方法の一つである．送信前に指定したPOP3サーバにあらかじめアクセスさせることによって，SMTPサーバの使用許可を与える方式．SMTPにはユーザ認証機能が過去には無かったため，管理外のネットワークからSMTPを利用させたい場合に使用してきた．

エ：不正な発信元からの電子メール受信を防ぐための方法の一つ．実在しないドメインから大量の広告電子メールが発信された場合に対する対策である．

問16　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 17

正解 □ 完璧 □ 直前CHECK □

無線LANで用いられるSSIDの説明として，適切なものはどれか．

ア　48ビットのネットワーク識別子であり，アクセスポイントのMACアドレスと一致する．

イ　48ビットのホスト識別子であり，有線LANのMACアドレスと同様の働きをする．

ウ　最長32オクテットのネットワーク識別子であり，接続するアクセスポイントの選択に用いられる．

エ　最長32オクテットのホスト識別子であり，ネットワーク上で一意である．

問 18

正解 □ 完璧 □ 直前CHECK □

シリアル回線で使用するものと同じデータリンクのコネクション確立やデータ転送を，LAN上で実現するプロトコルはどれか．

ア　MPLS　　イ　PPP　　ウ　PPPoE　　エ　PPTP

問 19

正解 □ 完璧 □ 直前CHECK □

ネットワーク管理プロトコルであるSNMPバージョン1のメッセージタイプのうち，事象の発生をエージェント自身が自発的にマネージャに知らせるために使用するものはどれか．

ア　get-request　　イ　get-response　　ウ　set-request　　エ　trap

問17　ウ

SSID（Service Set ID）：アクセスポイント内で同じグループ識別子をもつ端末同士だけが通信できるように，アクセスを制限するIDである．

ア：**BSSID**（Basic Service Set Identifier）の説明である．

イ：SSIDはアクセスポイントのグループであるため，有線LANのように自端末を識別するものではない．

エ：SSIDはホスト識別子ではない．**ネットワーク識別子**である．

問18　ウ

MPLS（Multi Protocol Label Switching）：主にWANで使用されるL3スイッチングである．ルーティング情報にラベルを付けることでルーティングを高速化する．

PPP（Point to Point Protocol）：ダイヤルアップによるISPへの接続などに用いられるデータリンク層プロトコルである．認証機能やデータ圧縮機能等を備えている．

PPPoE（PPP over Ethernet）：PPP（Point To Point Protocol），つまりダイヤルアップなどに使われるプロトコルをイーサネット上でトンネリングするもので，ADSLの接続などに利用されている．

PPTP（Point to Point Tunneling Protocol）：ダイヤルアップ回線で，TCP/IP などのプロトコルをトンネリングするプロトコルである．

問19　エ

SNMP（Simple Network Management Protocol）は，LANの構成機器の動作をネットワーク管理者が把握できるように，機器の状態を監視するプロトコルである．ネットワーク上にあるスイッチングハブやルータなどの管理対象を**SNMPエージェント**と呼び，**SNMPマネージャ**で一括管理する．管理対象の機器は，管理情報データベース**MIB**（Management Information Base）を持つ．

ネットワーク機器の状況の変化をSNMPマネージャに通知するために**Trap**が用いられる．Trapは，マネージャからの問合せがなくても，機器の状態が変化したときにエージェントから通知される．

get-request：SNMPエージェントに情報取得を要求するメッセージタイプ．

get-response：SNMPマネージャからの要求に応答するメッセージタイプ．

set-request：SNMPエージェントに情報変更を要求するメッセージタイプ．

trap：自発的に事象をSNMPマネージャに通知するメッセージタイプ．

問題

問 20

正解 完璧 直前CHECK

WebDAVの特徴はどれか.

ア　HTTP上のSOAPによってソフトウェア同士が通信して，ネットワーク上に分散したアプリケーションを連携させることができる.

イ　HTTPを拡張したプロトコルを使って，サーバ上のファイルの参照や作成，削除及びバージョン管理が行える.

ウ　WebアプリケーションからIMAPサーバにアクセスして，ブラウザから添付ファイルを含む電子メールの操作ができる.

エ　ブラウザで“ftp://”から始まるURLを指定して，ソフトウェアなどの大容量ファイルのダウンロードができる.

問 21

正解 完璧 直前CHECK

SQLのGRANT文による権限定義に関する記述のうち，適切なものはどれか.

ア　PUBLIC指定によって，全ての権限を与えることができる.

イ　WITH GRANT OPTION指定によって，権限を付与可能にすることができる.

ウ　ビューに対して固有の参照権限を定義できない.

エ　表定義のSQL文内にGRANT文を指定することによって，権限定義ができる.

問20　イ

WebDAV（Web Distributed Authoring and Versioning）：Webコンテンツの編集や管理を目的としたHTTPを拡張し，クライアント（Webブラウザ）からWebサーバ上のファイルやフォルダを管理できるようにした仕様．HTTP 1.1 を拡張した仕様で，IETFによってRFC2518として定義されている．HTTPの拡張仕様であるため，SSLによる暗号化はHTTPS上でWebDAVを利用するだけでよい．

問21　イ

SQLにおける**GRANT文**は，アクセス権の定義に用いられる．GRANTで指定できる権限は表のとおりである．逆に，アクセス権を削除する場合は，**REVOKE文**を利用する．

SELECT	任意の列に対する選択を許可
INSERT	新規行の追加を許可
UPDATE	列に対する更新を許可
DELETE	行の削除を許可
RULE	ルールの作成を許可
REFERENCES	外部キー参照制限を持つテーブルへの権限許可
TRIGGER	トリガの作成許可
ALL PRIVILEGES	上の7つの権限を一度に許可

ア：すべての権限は，**ALL PRIVILEGES**によって与えることができる．
イ：正しい．**WITH GRANT OPTION**により権限を与えられたユーザがさらにその権限を他のユーザに与えることができる．
ウ：固有の参照権限を定義できるため誤りである．

問題

問 22

正解 完璧 直前CHECK

システム開発で行われる各テストについて，そのテスト要求事項が定義されるアクティビティとテストの組合せのうち，適切なものはどれか．

	システム方式設計	ソフトウェア方式設計	ソフトウェア詳細設計
ア	運用テスト	システム結合テスト	ソフトウェア結合テスト
イ	運用テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
ウ	システム結合テスト	ソフトウェア結合テスト	ソフトウェアユニットテスト
エ	システム結合テスト	ソフトウェアユニットテスト	ソフトウェア結合テスト

問 23

正解 完璧 直前CHECK

開発した製品で利用している新規技術に関して特許の出願を行った．日本において特許権の取得が可能なものはどれか．

ア　学会で技術内容を発表した日から11か月目に出願した．
イ　顧客と守秘義務の確認を取った上で技術内容を説明した後，製品発表前に出願した．
ウ　製品に使用した暗号の生成式を出願した．
エ　製品を販売した後に出願した．

問 24

正解 完璧 直前CHECK

ITサービスマネジメントの情報セキュリティ管理プロセスに対して，JIS Q 20000-1が要求している事項はどれか．

ア　潜在的な問題を低減させるために，予防処置を取らなければならない．
イ　ディジタルの構成品目の原本を，物理的又は電子的にセキュリティが保たれた書庫で管理しなければならない．
ウ　変更要求に対しては，そのリスク，影響及び事業利益について，アセスメントを行わなければならない．
エ　変更を実装する前に，変更がセキュリティ管理策に与える影響のアセスメントを行わなければならない．

問22 ウ

システム開発では，以下の順番で設計からテストまでが行われる．

システム方式設計→ソフトウェア方式設計→ソフトウェア詳細設計→ソフトウェアユニットテスト→ソフトウェア結合テスト→システム結合テスト→運用テスト

システム方式設計：システム全体の方式設計．

ソフトウェア方式設計：システムを構成するソフトウェアの方式設計．

ソフトウェア詳細設計：ソフトウェアをユニットに分け，各ユニットを詳細に設計する．

ソフトウェアユニットテスト：ソフトウェア詳細設計をもとに開発したユニットを動作確認するテスト．

ソフトウェア結合テスト：それぞれのユニットを結合してソフトウェアを動作確認するテスト．

システム結合テスト：システム全体について，その目的や機能，応答時間や負荷をかけたときの性能などが目標に達しているかを確認するテスト．開発の最終確認である．

運用テスト：システムの利用者や運用する担当者の主導で行われるテスト．利用部門が用意したデータを用いた承認テストなどがある．

問23 イ

ア，エ：特許取得では，次の条件の発明は受け付けられない．

・特許出願前に日本国内又は外国において公然知られた発明

・特許出願前に日本国内又は外国において公然実施をされた発明

・特許出願前に日本国内又は外国において頒布された刊行物に掲載された発明

ウ：特許権取得では，自然法則を利用した技術的思想の創作のうち高度なものを保護対象とするため，計算方法や暗号等の自然法則の利用が無いものは対象とならない．

問24 エ

ア：JIS Q 20000-1 8.3 問題管理に要求事項が定義されている．

イ：JIS Q 20000-1 9.1 構成管理に要求事項が定義されている．

ウ：JIS Q 20000-1 9.2 変更管理に要求事項が定義されている．

エ：JIS Q 20000-1 6.6 情報セキュリティ管理に要求事項が定義されている．

問 25　正解　完璧　直前CHECK

内部監査として実施したシステム監査で，問題点を検出後，改善勧告を行うまでの間に監査人が考慮すべき事項として，適切なものはどれか．

ア　改善事項を被監査部門へ事前に通知した場合，不備の是正が行われ，元から不備が存在しなかったように見える可能性があるので，被監査部門に秘匿する．

イ　監査人からの一方的な改善提案は実行不可能なものとなるおそれがあるので，改善勧告の前に，改善策について被監査部門との間で協議する場をもつ．

ウ　経営判断に関与することを避けるため，不備を改善する際の経済合理性などの判断を行わず，そのまま経営者に対する改善勧告とする．

エ　将来のフォローアップに際して，客観的で中立的な判断を阻害する要因となるので，改善勧告の優先度付けや取捨選択を行うことを避ける．

問25　イ

ア：被監査部門への通知は監査後に行われるものであるため，不備の是正が行われても不備が存在しなかったことにはならない．

イ：正しい．監査人は中立的な立場で改善提案を行うが，被監査部門の事情を考慮した改善提案を行う必要がある．そのため，協議によって実行可能な対応を改善勧告を調整する．

ウ：たとえ不備があったとしても，経済合理性がなければ対処できない．被監査部門，経営者へ報告し協議するほうが良い．

エ：改善勧告は，妥当性を有する必要がある．そのため，優先度付けや取捨選択を行い，具体的な改善案を提示する必要がある．