問題

問 1

正解 □ 完璧 □ 直前CHECK □

DNSキャッシュポイズニングに分類される攻撃内容はどれか.

ア　DNSサーバのソフトウェアのバージョン情報を入手して，DNSサーバのセキュリティホールを特定する.

イ　PCが参照するDNSサーバに誤ったドメイン管理情報を注入して，偽装されたWebサーバにPCの利用者を誘導する.

ウ　攻撃対象のサービスを妨害するために，攻撃者がDNSサーバを踏み台に利用して再帰的な問合せを大量に行う.

エ　内部情報を入手するために，DNSサーバが保存するゾーン情報をまとめて転送させる.

問 2

正解 □ 完璧 □ 直前CHECK □

SSLを使用して通信を暗号化する場合，SSL-VPN装置に必要な条件はどれか.

ア　SSL-VPN装置は，1台1台を識別できるようにディジタル証明書を組み込む必要がある.

イ　SSL-VPN装置は，装置メーカが用意した機種固有のディジタル証明書を組み込む必要がある.

ウ　SSL-VPN装置は，装置メーカから提供される認証局を利用する必要がある.

エ　同一ドメイン内で複数拠点にSSL-VPN装置を設置する場合は，同一のディジタル証明書を利用する必要がある.

問1　イ

DNSサーバにはコンテンツサーバとキャッシュサーバの2種類ある．

コンテンツサーバ：ドメイン情報を管理している．

キャッシュサーバ：クライアントに代わってコンテンツサーバにドメイン情報の問合せ行い，その回答結果をクライアントに返してキャッシュに格納する．もし，クライアントの問合せに対してキャッシュが存在していれば，キャッシュされたドメイン情報を返す．

DNSキャッシュポイズニングは，本物のコンテンツサーバからの回答よりも先に偽の回答を送り込むことで，キャッシュサーバに偽の情報をキャッシュさせる攻撃である．キャッシュサーバに偽のドメイン情報がキャッシュされてしまうと，キャッシュサーバがクライアントに偽のドメイン情報を返してしまい，クライアントが偽装されたWebサーバに誘導されてしまう．

問2　ア

SSL-VPNは，トランスポート層のデータを暗号化して送受信する暗号通信プロトコルである**SSL**（Secure Socket Layer）を用いて，インターネット網をあたかも専用回線であるかのように利用する**VPN**（Virtual Private Network）を構築する暗号通信方式である．

イ：SSL-VPN装置のディジタル証明書は，メーカが用意したものでなく認証局から装置に対して発行されたディジタル証明書を用いる．

ウ：装置メーカから提供される認証局を利用する必要はない．

エ：SSL-VPN装置は，異なるディジタル証明書を利用する．

問題

問 3

正解 □ 完璧 □ 直前CHECK □

シングルサインオンの説明のうち，適切なものはどれか．

ア　クッキーを使ったシングルサインオンの場合，サーバごとの認証情報を含んだクッキーをクライアントで生成し，各サーバ上で保存，管理する．

イ　クッキーを使ったシングルサインオンの場合，認証対象の各サーバを異なるインターネットドメインに配置する必要がある．

ウ　リバースプロキシを使ったシングルサインオンの場合，認証対象の各Webサーバをそれぞれ異なるインターネットドメインにする必要がある．

エ　リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル照明書を用いることができる．

問 4

正解 □ 完璧 □ 直前CHECK □

スパムメールの対策として，あて先ポート番号25番のメールに対し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受信メールのうち，スパムメールのシグネチャに該当するメールを遮断する．

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に直接送信されたメールを遮断する．

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メールを遮断する．

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受信メールを遮断する．

問3　エ

シングルサインオン（SSO：Single Sign-On）とは，ユーザが一度認証を受けるだけで，許可されているすべての機能を利用できるようになる機能のことである．認証対象ごとにIDとパスワードを入力する手間を省くことができ，ユーザが記憶しておく必要のあるID・パスワードの数を減らすこともできる．

ア：クッキーはクライアント上に保存される．

イ，ウ：認証対象のサーバは同じインターネットドメインでもよい．

エ：ディジタル証明書やその他の認証要素（認証トークン，ICカードなど）に対応したシステムもある．

問4　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．

問題

問 5

正解 □ 完璧 □ 直前CHECK □

ディジタル署名を利用する目的はどれか.

ア　受信者が署名鍵を使って暗号文を元の平文に戻すことができるようにする.
イ　送信者が固定文字列を付加した平文を署名鍵を使って暗号化し，受信者がメッセージの改ざん部位を特定できるようにする.
ウ　送信者が署名鍵を使って署名を作成し，それを平文に付加することによって，受信者が送信者を確認できるようにする.
エ　送信者が署名鍵を使って平文を暗号化し，平文の内容を関係者以外に分からないようにする.

問 6

正解 □ 完璧 □ 直前CHECK □

SHA-1を説明したものはどれか.

ア　160ビットの出力データを生成し，改ざんの検出に利用するアルゴリズム
イ　IPsecで使用される暗号化アルゴリズム
ウ　公開鍵暗号方式において暗号化鍵を生成するアルゴリズム
エ　データの暗号化が正常に完了したことの確認に利用するアルゴリズム

問 7

正解 □ 完璧 □ 直前CHECK □

リスク対策をリスクコントロールとリスクファイナンスに分けた場合，リスクファイナンスに該当するものはどれか.

ア　システムが被害を受けた場合を想定して保険をかけた.
イ　システム被害につながるリスクの発生を抑える対策に資金を投入した.
ウ　システムを復旧するのに掛かった費用を金融機関から借り入れた.
エ　リスクが顕在化した場合のシステム被害を小さくする対策に資金を投入した.

問5　ウ

ディジタル署名とは，電子文書の送信者の正当性と電子文書の非改ざん性を保証するために付加された，暗号化された署名情報である．送信者は，自身の秘密かぎ（署名かぎ）で暗号化した署名を電子文書に付加して送る．受信者は，送信者の公開かぎを用いて署名を復号して，正しい内容かどうかを確認する．また，第三者によって電子文書が改ざんされていないか，偽造されたものでないかを確認することもできる．

ア，エ：**署名鍵**は暗号通信を目的にした鍵でない．

イ：**ディジタル署名**では平文に固定文字列を付加しない．

問6　ア

SHA-1はハッシュ関数のアルゴリズムであり，入力したメッセージから160ビットのハッシュ値を出力する．データの送受信において，送信前と受信後のメッセージのハッシュ値を比較することにより，通信経路の途中で改ざんを検出することができる．

イ：SHA-1はIPSecにおいてハッシュ関数として使用される．

ウ：暗号化鍵の生成には，擬似乱数を生成するアルゴリズムが使用される．SHA-1はメッセージダイジェスト（ハッシュ値）を生成するアルゴリズムである．

エ：データの暗号化が正常に完了したことを確認するアルゴリズムではないため，暗号化データを復号して確認するしかない．

問7　ア

リスク対策は，一般的にリスクの回避・軽減・移転・保有の四つの手法が考えられる．**リスクファイナンス**とは，そのうちリスクの保有と移転に関わる手法を示し，リスクが現実に発生した際の損失の補償を準備することである．

リスクの保有は自らの組織で対処することであり，リスクの移転は保険の契約等を通じて第三者へリスクを移転することである．

イ，エ：リスクファイナンスはリスクが発生した場合の対策である．

ウ：リスクファイナンスは損失の補償を準備することである．

問題

問 8

正解 □ 完璧 □ 直前CHECK □

情報システムのリスク分析に関する記述のうち，適切なものはどれか．

ア　リスクには，投機的リスクと純粋リスクとがある．情報セキュリティのためのリスク分析で対象とするのは，投機的リスクである．

イ　リスクの予想損失額は，損害予防のために投入されるコスト，復旧に要するコスト，及びほかの手段で業務を継続するための代替コストの合計で表される．

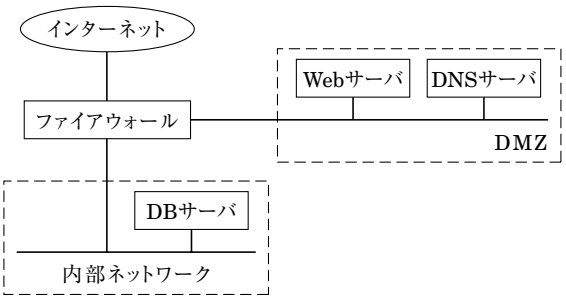
ウ　リスク分析では，現在に発生すれば損失をもたらすリスクが，情報システムのどこに，どのように潜在しているかを識別し，その影響の大きさを測定する．

エ　リスクを金額で測定するリスク評価額は，損害が現実のものになった場合の1回当たりの平均予想損失額で表される．

問 9

正解 □ 完璧 □ 直前CHECK □

DMZ上の公開Webサーバで入力データを受け付け，内部ネットワークのDBサーバにそのデータを蓄積するシステムがある．DBサーバへの不正侵入対策の一つとして，ファイアウォールの最も有効な設定はどれか．



ア　DBサーバの受信ポートを固定にし，WebサーバからDBサーバの受信ポートへ発信された通信だけをファイアウォールで通す．

イ　DMZからDBサーバあての通信だけをファイアウォールで通す．

ウ　Webサーバの発信ポートは任意のポート番号を使用し，ファイアウォールでは，いったん終了した通信と同じ発信ポートを使った通信を拒否する．

エ　Webサーバの発信ポートを固定し，その発信ポートの通信だけをファイアウォールで通す．

問8　ウ

リスク分析とは，企業や対象となる情報システムの**機密性**，**保全性**，**可用性**を阻害する様々なリスクを洗い出し，その影響度を分析することである．脅威と脆弱性が結びつくとリスクが顕在化し，損失が発生する．

ア：情報システムにおけるリスクマネジメントでは，主に純粋リスクを対象として取り扱う．

イ：リスクの予想損失額は，セキュリティ侵害が発生してから元の状態に戻るまでにかかる費用となる．また，損害のために失ったビジネスチャンスや損害そのもののコストを含める必要がある．

エ：リスク評価額は，「1回当たりの予想損失額×発生頻度（回数／年）」で表せる．

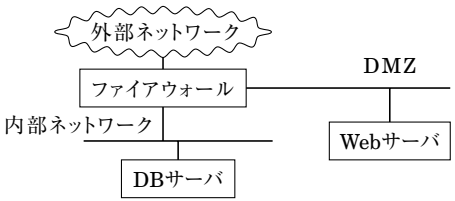
問9　ア

ファイアウォールは，内部ネットワークと外部ネットワークの間に設置される．内部ネットワークの情報システムを保護するために，セキュリティポリシに従った設定ルールによって内部ネットワークと外部ネットワークの間を通過しようとするパケットを制御する．

問題文から，内部ネットワークのDBサーバを外部ネットワークから保護し，DBサーバと連携するDMZ上のWebサーバからの通信を許可する設定を選択すればよい．

イ，ウ：Webサーバの発信ポートではなく，DBサーバの受信ポートの設定でなければ，DBサーバを保護する設定とならない．

エ：この設定では，外部ネットワークからDBサーバにパケットが到達してしまう．



問題

問 10

正解 □ 完璧 □ 直前CHECK □

通信の暗号化に関する記述のうち，適切なものはどれか．

ア　IPsecのトランスポートモードでは，ゲートウェイ間の通信経路上だけではなく，発信ホストと受信ホストとの間の全経路上でメッセージが暗号化される．

イ　LDAPクライアントがLDAPサーバに接続するとき，その通信内容は暗号化することができない．

ウ　S/MIMEで暗号化した電子メールは，受信側のメールサーバ内に格納されている間は，メール管理者が平文として見ることができる．

エ　SSLを使用すると，暗号化されたHTML文書はブラウザでキャッシュの有無が設定できず，ディスク内に必ず保存される．

問 11

正解 □ 完璧 □ 直前CHECK □

メールサーバ（SMTPサーバ）の不正利用を防止するために行う設定はどれか．

ア　ゾーン転送のアクセス元を制御する．

イ　第三者中継を禁止する．

ウ　ディレクトリに存在するファイル名の表示を禁止する．

エ　特定のディレクトリ以外でのCGIプログラムの実行を禁止する．

問 12

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か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などに不正に組み込んだものを隠ぺいする機能をまとめたツール

問10　ア

ア：**IPSec**の**トランスポートモード**では，End-to-Endでメッセージを暗号通信するため，ゲートウェイ間の通信経路上だけでなく，発信側システムと受信側システムとの間の全経路上でメッセージが暗号化されている．

イ：**LDAP**では，**TLS**や**SSL**を用いた暗号通信について標準化されている．

ウ：**S/MIME**では，送信者が電子メールのメッセージを暗号化し，受信者がメッセージを復号するため，メールサーバ内に格納されている間もメッセージが暗号化されている．

エ：**SSL**を使用した場合においては，ブラウザでキャッシュの有無が設定できないことや，暗号化されたHTMLデータがディスク内に必ず保存されることについて，何も規定していない．

問11　イ

メールサーバでは，SPAMメールや迷惑メールの中継防止として，メールサーバの管理外の第三者からのメールの中継を禁止する必要がある．ただし，運用の都合で第三者中継を一律に禁止できない場合には，個別のアドレスやドメインからのメールのみを許可するように設定する．

ア：DNSサーバの不正防止対策である．

ウ：FTPサーバの不正防止対策である．

エ：Webサーバの不正防止対策である．

問12　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．

問題

問 13

正解 □ 完璧 □ 直前CHECK □

TCP/IPのネットワークにおけるICMPの説明として，適切なものはどれか．

ア　MACアドレスだけが分かっているときにIPアドレスの解決を可能にする．
イ　グローバルIPアドレスとプライベートIPアドレスを相互に変換する．
ウ　送信元ホストへ，IPパケットの送信エラー報告などの制御メッセージを通知する．
エ　ネットワーク内のIPアドレスを一元管理し，クライアントに動的に割り当てる．

問 14

正解 □ 完璧 □ 直前CHECK □

TCP/IPのネットワークにおいて，TCPのコネクションを識別するために必要なものの組合せはどれか．

ア　あて先IPアドレス，あて先TCPポート番号
イ　あて先IPアドレス，あて先TCPポート番号，送信元IPアドレス，送信元TCPポート番号
ウ　あて先IPアドレス，送信元IPアドレス
エ　あて先MACアドレス，あて先IPアドレス，あて先TCPポート番号，送信元MACアドレス，送信元IPアドレス，送信元TCPポート番号

問 15

正解 □ 完璧 □ 直前CHECK □

TCPヘッダ中のウィンドウサイズの説明として，適切なものはどれか．

ア　受信エラー時の再送に備えて送信側が保持しているデータのサイズを受信側に知らせるために使用される．
イ　受信側からの確認応答を待たずに，データを続けて送信できるかどうかの判断に使用される．
ウ　送信側と受信側の最適なバッファサイズを接続開始時のハンドシェイクで決定するために使用される．
エ　複数セグメントから成るデータの送信時，後続するセグメント数を受信側に知らせるために使用される．

問13　ウ

ア：**RARP**（Reverse Address Resolution Protocol）の説明である．
イ：**ICMP**（Internet Control Message Protocol）の説明である．
ウ：**NAT**（Network Address Translation）の説明である．
エ：**DHCP**（Dynamic Host Configuration Protocol）の説明である．

問14　イ

TCP/IPのネットワークは，あて先IPアドレス，あて先ポート番号と送信元IPアドレス，送信元ポート番号の組でコネクションを構築する．IPアドレスで相手のマシンが指定され，ポート番号で接続するアプリケーションが指定される．

問15　イ

TCPでは，送信側が確認応答を待たずに送信できるデータの大きさを**ウィンドウサイズ**という．受信側が送信側に受信可能なデータサイズを通知するようになっている．

受信側が送信側にウィンドウサイズを通知することで，受信側がデータを取りこぼさない大きさのデータサイズでデータを送信し，データの再送を発生させない，効率のよい通信を行う．

問題

問 16

正解 □ 完璧 □ 直前CHECK □

RDBMSの表へのアクセスにおいて，特定の利用者だけにアクセス権を与える方法として，適切なものはどれか．

ア　CONNECT文で接続を許可する．
イ　CREATE ASSERTION文で表明して制限する．
ウ　CREATE TABLE文の参照制約で制限する．
エ　GRANT文で利用を許可する．

問 17

正解 □ 完璧 □ 直前CHECK □

DBMSの排他制御機能に関する記述のうち，適切なものはどれか．

ア　排他制御機能によって，同時実行処理でのデータの整合性を保つことができる．
イ　排他制御機能の使用によって，デッドロックを防止できる．
ウ　排他制御はDBMSが自動的に行い，アプリケーションプログラムからロック，アンロックの指示はできない．
エ　バッチによる更新処理では排他制御を行う必要はない．

問 18

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16　エ

CONNECT：DBMSとの接続に用いる．
CREATE ASSERTION：データ操作時の条件を設定するために用いる．
CREATE TABLE：参照先の整合性を確認するために用いる．
GRANT：特定のデータベース利用者に特定の作業を行う権限を与えるために用いる．

問17　ア

DBMSの排他制御機能とは，同じデータを同時に更新することによるデータの矛盾の発生が起こらないように，**セマフォ**などを利用して書込みを一時的に制限すること．
イ：**デッドロック**は，排他制御機能により発生する．デッドロックを避ける手法としては，データの更新順序を決めておく，排他制御をかける範囲を狭くする，などある．
ウ：DBMSが自動的に行うものと，アプリケーションプログラムがDBMSに明示的に指示して行うものとがある．
エ：複数のバッチ処理を同時に行う場合には，排他処理が必要となる．

問18　ウ

システム開発では，
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
の順番で行われる．
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．

問題

問 19

正解 □ 完璧 □ 直前CHECK □

ハードウェアの保守点検及び修理作業を実施するときに，運営管理者が実施すべき，事前又は事後の確認に関する説明のうち，適切なものはどれか．

ア　システムが自動的に回復処理を行った障害については，障害前後のエラーログが残っているので，障害原因や対応処置の報告ではなく，ログの分析結果を確認する．
イ　定期保守時の点検項目は事前に分かっているので，事前と事後の確認は省略できるが，作業の開始と終了については，保守作業者に確認する．
ウ　予防保守を遠隔保守方式で行う場合，遠隔地のシステムへの影響は出ないので，作業内容などの事前確認は行わず，事後に作業実施結果を確認する．
エ　臨時保守の場合，事前に保守作業者が障害の発生状況を確認したことを確認し，事後に障害原因や作業実施結果を確認する．

問 20

正解 □ 完璧 □ 直前CHECK □

ソフトウェア開発のプロセスモデルのうち，開発サイクルを繰り返すことによって，システムの完成度を高めていくプロセスモデルはどれか．

ア　RADモデル
イ　ウォータフォールモデル
ウ　スパイラルモデル
エ　プロトタイピングモデル

問 21

正解 □ 完璧 □ 直前CHECK □

ソフトウェアを保守するときなどに利用される技術であるリバースエンジニアリングの説明はどれか

ア　ソースプログラムを解析してプログラム仕様書を作る．
イ　ソースプログラムを探索して修正箇所や影響度を調べる．
ウ　ソースプログラムを見直して構造化プログラムに変換する．
エ　ソースプログラムを分かりやすい表現に書き換える．

問19　エ

保守作業には大きく分けて，**定期保守**と**臨時保守**の二つがある．定期保守は，決まった間隔でシステムに異常の兆候は見られないかを確認するものである．点検事項もあらかじめ決められた項目について確認する．臨時保守は，定期保守でなんらかの不具合を見つけた場合や，保守以外で不具合を見つけた場合に実施する作業である．作業の着手前に状況確認と連絡を行い，処置後に原因の報告を実施する．

ア：システムが自動回復処置をとった障害は，事前に確認することはできない．

イ：事前に点検項目が決まっている定期保守でも，事後の確認は必要である．

ウ：予防保守は，遠隔保守であるかどうかに関わらず，事前報告を行う必要がある．

問20　ウ

RAD（Rapid Application Development）モデル：プログラミングの自動化，GUIの設計等を高機能な開発環境で行うことによって，ソフトウェアを短時間で簡単に開発する手法．

ウォータフォールモデル：基本計画，外部設計，内部設計，プログラム設計，プログラミング，テストの各工程を，滝が流れるように上流から下流へと進めていく手法．

スパイラルモデル：システムの変更可能な部分について，ユーザの要求に対応しながら成長させていく手法．

プロトタイピングモデル：試作品（プロトタイプ）を作り，ユーザの評価を得て改善しながら仕様を完成させていく手法．

問21　ア

実装済みのソフトウェアから設計仕様などを抽出して，そのソフトウェアの修正や再開発を支援したり，他社製品を分析・調査してその情報を利用したりすることを**リバースエンジニアリング**という．

エ：**リファクタリング**に関する記述である．

問題

問 22

正解 □ 完璧 □ 直前CHECK □

ITILにおけるインシデント管理プロセスの役割として，適切なものはどれか．

ア　新しいサービスの要求を利用者から受け付け，企画立案すること
イ　一時的回避策で対処した問題を分析し，恒久対策を検討すること
ウ　潜在的な問題を事前に発見し，変更要求としてとりまとめること
エ　低下したサービスレベルを回復させ，影響を最小限に抑えること

問 23

正解 □ 完璧 □ 直前CHECK □

データベースサーバのハードディスクに障害が発生した場合でもサービスを続行できるようにするための方策として，最も適切なものはどれか．

ア　共通データベースの格納場所を複数のハードディスクに分散させる．
イ　サーバのディスクを二重化し，通常稼働時は同時に二つのディスクに書き込む．
ウ　サーバの予備機を設置し，OSとアプリケーションソフトを本番機と同じ構成にして待機させておく．
エ　別のディスクにデータベースを毎週末にコピーする．

問 24

正解 □ 完璧 □ 直前CHECK □

アクセス権限を管理しているシステムの利用者IDリストから，退職による権限喪失者が削除されていることを検証する手続として，最も適切なものはどれか．

ア　アクセス権限削除申請書の全件について，利用者IDリストから削除されていることを確認する．
イ　最新の利用者IDリストの全件について対応するアクセス権限削除申請書が存在しないことを確認する．
ウ　人事発令簿の退職者の全件について，利用者IDリストから削除されていることを確認する．
エ　利用者IDリストの更新履歴の全件について，対応するアクセス権限削除申請書の存在を確認する．

問22　エ

ITILのインシデント管理では，インシデントに対して速やかに対処し，回復させて，サービスへの影響を最小限に抑える処理を行う．

インシデントとは，サービスの品質を阻害，または阻害する可能性のある事象のことをいう．一方，**ITIL**（IT Infrastructure Library）は，システム管理・運用規則に関するガイドラインである．ITサービスとは従来の運用管理，保守管理のことで，その**サービスマネジメント**は**サービスサポート**と**サービスデリバリ**の二つに分類される．

サービスデリバリ：サービスレベル管理，キャパシティ管理，可用性管理，ITサービス財務管理，ITサービス継続性管理

サービスサポート：サービスデスク，インシデント管理，問題管理，構成管理，変更管理，リリース管理

問23　イ

ア：複数に分散したハードディスクの一つに障害が発生した場合に，そのハードディスクを使用していたサービスは継続できなくなる．

イ：二重化している片方のハードディスクに障害が発生した場合でも，もう一方のハードディスクが稼働しているため，サービスを継続できる．

ウ：ハードディスク障害発生から予備機稼働までの間，システムが停止するため，サービスが継続できなくなる．

エ：ハードディスク障害発生から別ディスクを用いてデータベースのデータを回復するまでシステムが停止するため，サービスが継続できなくなる．

問24　ウ

アクセス権限削除申請書は，本人または部門責任者から提出されることを考えると，申請を忘れる可能性が考えられるため，退職による権限喪失者の削除検証手続きの利用に適切でない．

一方，**人事発令簿**は退職者に漏れがないため，退職による権限喪失者の削除検証手続きの利用に適切である．

問題

問 25

正解 □ 完璧 □ 直前CHECK □

外部保管のために専門業者にバックアップ媒体を引き渡す際の安全性について，セキュリティ監査を実施した．指摘事項となる状況はどれか．

ア　委託元責任者が，一定期間ごとに，専門業者における媒体保管状況を確認している．

イ　委託元責任者が，専門業者との間で，機密保持条項を盛り込んだ業務委託契約を結んだ上で引き渡している．

ウ　委託元担当者が，専用の記録簿に，引渡しの都度，日付と内容を記入し，専門業者から受領印をもらっている．

エ　委託元担当者が，バックアップ媒体を段ボール箱に入れ，専門業者に引き渡している．

問25　エ

バックアップ媒体を引き渡す際にリスクとなりうる事項に対処していないと，**指摘事項**となる．

ア：専門業者が適切に媒体を保管していないと想定すると，一定期間ごとに媒体の保管状況を確認することは適切な対処である．

イ：専門業者にバックアップ媒体を渡すことから，**業務委託契約**に**秘密保持条項**を盛り込むことで適切に対処している．

ウ：専門業者に引渡ししたバックアップ媒体の紛失や盗難に会うことを想定すると，引渡し記録をとって専門業者から受領印をもらうことは適切な対処である．

エ：委託元担当者が，専門業者にバックアップ媒体について何も確認せず渡していることが指摘事項となる．