問 1 正解 完璧 直前チェック

RADIUSやDIAMETERが提供するAAAフレームワークの構成要素は，認証（Authentication）及び認可（Authorizarion）の他にどれか。

ア Accounting　　イ Activation
ウ Audit　　エ Augmented Reality

問 2 正解 完璧 直前チェック

NTPリフレクション攻撃の特徴はどれか。

ア 攻撃対象であるNTPサーバに高頻度で時刻を問い合わせる。
イ 攻撃対象であるNTPサーバの時刻情報を書き換える。
ウ 送信元を偽って，NTPサーバにecho requestを送信する。
エ 送信元を偽って，NTPサーバにレスポンスデータが大きくなる要求を送信する。

問1 ア

解説

DIAMETER：RADIUSの後継プロトコルとしてRFC 3588として策定された。RADIUSが作られた当初には，想定されていなかったネットワークの増大化に関して，機能や制限が拡張されている。AAAフレームワークの構成要素は，認証（**Authentication**），認可（**Authorization**），課金（**Accounting**）となっている。

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を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）と認証機能を分離することで，利用者の一元管理と，アクセスログの記録が可能となる。

RADIUSとDIAMETERの比較の一部

	RADIUS	DIAMETER
プロトコル	UDPのみ	TCP or SCTP
同時接続数	256	40億以上
通信の方向性	片方向	双方向
冗長化	定義なし	定義あり

問2 エ

解説 **NTPリフレクション攻撃**は，NTPサーバに対して送信元を偽り問合せを行うことで，レスポンスデータが大きくなる要求を利用した攻撃手法である。具体的には，NTPサーバに対して過去に通信したサーバのリストを要求すると，数百台のIPアドレスを返送する。この機能を利用し，返送先IPアドレスを攻撃対象に偽装し，多数のDNSサーバへリスト要求をすることで，返信されたリストのトラフィックにより攻撃対象をダウンさせる攻撃である。

問 3 正解 完璧 直前チェック

POODLE（CVE-2014-3566）攻撃の説明はどれか。

ア　SSL 3.0のサーバプログラムの脆弱性を突く攻撃であり，サーバのメモリに不正アクセスして秘密鍵を窃取できる。
イ　SSL 3.0を使用した通信において，ブロック暗号のCBCモード利用時の脆弱性を突く攻撃であり，パディングを悪用して暗号化通信の内容を解読できる。
ウ　TLS 1.2のプロトコル仕様の脆弱性を突く攻撃であり，TLSの旧バージョンにダウングレードして暗号化通信の内容を解読できる。
エ　TLS 1.2を使用した通信において，Diffie-Hellman鍵交換アルゴリズムの脆弱性を突く攻撃であり，交換されたセッション鍵を窃取して暗号化通信の内容を解読できる。

問 4 正解 完璧 直前チェック

XMLディジタル署名の特徴のうち，適切なものはどれか。

ア　XML文書中の，任意のエレメントに対してデタッチ署名（Detached Signature）を付けることができる。
イ　エンベロープ署名（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 5 正解 完璧 直前チェック

ファイアウォールにおけるダイナミックパケットフィルタリングの特徴はどれか。

ア　IPアドレスの変換が行われるので，ファイアウォール内部のネットワーク構成を外部から隠蔽できる。
イ　暗号化されたパケットのデータ部を復号して，許可された通信かどうかを判断できる。
ウ　パケットのデータ部をチェックして，アプリケーション層での不正なアクセスを防止できる。
エ　戻りのパケットに関しては，過去に通過したリクエストパケットに対応付けられるものだけを通過させることができる。

問3 イ

解説 **POODLE**（Padding Oracle On Downgraded Legacy Encryption）は，SSL 3.0通信のPadding（パディング）脆弱性をついた攻撃である。**パディング**とは，短いデータの前や後に無意味なデータを追加して長さを合わせる処理のことである。

POODLEでは，SSL 3.0におけるブロック暗号上のパディングの検証に脆弱性がある。このパディングは，プロトコルによって検証されないため，攻撃者は任意データをパディングとして利用し，そこから1つ前のデータを繰り返し推測することで，暗号化された通信を1バイトずつ平文に復号し入手することができる。

また，POODLEではSSL/TLSのバージョンダウングレード（Downgraded Legacy Encryption）を利用する。クライアントからWebサーバへ，通信する際にTLS 1.2で通信を試み失敗した場合は，TLS 1.1で通信するといった，低いバージョンへのダウングレードによる通信確立の動作ロジックがある。この動作ロジックを悪用し，TLS 1.2での通信失敗，TLS 1.1，TLS 1.0，SSL 3.0というようにバージョンを下げた時点でパディングを利用しWebサーバとクライアント間の通信を解読する。

問4 ア

解説 **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のため，同じ文書に複数人の署名を付ける用途に適しているが，必ず複数の署名を付けるわけではない。
ウ：署名形式は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に比べてXMLディジタル署名は，XMLタグ付き言語のためわかりやすい。

問5 エ

解説 **ダイナミックパケットフィルタリング**は，ファイアウォールのパケット通過時のパケット開放の方式である。内部から外部への通信を実行した際に，外部からの戻りパケットもファイアウォールで開放する必要がある。ダイナミックパケットフィルタリングでは，戻りパケットを必要な状況に応じて動的に開放し，要求がない場合はポートを閉じておく方式である。

ア：IPアドレスの変換とは関係がない。
イ：パケットの暗号化とは関係がない。
ウ：パケットのデータ部分のチェックは行っていない。

問 6 正解 完璧 直前チェック

リスクベース認証に該当するものはどれか。

ア　インターネットからの全てのアクセスに対し，トークンで生成されたワンタイムパスワードで認証する。
イ　インターネットバンキングでの連続する取引において，取引の都度，乱数表の指定したマス目にある英数字を入力させて認証する。
ウ　利用者のIPアドレスなどの環境を分析し，いつもと異なるネットワークからのアクセスに対して追加の認証を行う。
エ　利用者の記憶，持ち物，身体の特徴のうち，必ず二つ以上の方式を組み合わせて認証する。

問 7 正解 完璧 直前チェック

X.509におけるCRL（Certificate Revocation List）についての説明のうち，適切なものはどれか。

ア　PKIの利用者は，認証局の公開鍵がWebブラウザに組み込まれていれば，CRLを参照しなくてもよい。
イ　認証局は，発行した全てのディジタル証明書の有効期限をCRLに登録する。
ウ　認証局は，発行したディジタル証明書のうち，失効したものは，失効後1年間CRLに登録するよう義務付けられている。
エ　認証局は，有効期限内のディジタル証明書をCRLに登録することがある。

問 8 正解 完璧 直前チェック

CRYPTRECの主な活動内容はどれか。

ア　暗号技術の安全性，実装性及び利用実績の評価・検討を行う。
イ　情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ対策の推進に係る企画などを行う。
ウ　組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。
エ　認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。

春 秋

問6 ウ

解説 **リスクベース認証**は，利用者のIPアドレスなど普段利用している環境を分析し，異なるネットワークからのアクセスに対して，追加認証を行う仕組みである。普段自宅から銀行のネットバンキングを利用している利用者が，海外でネットバンキングに接続した場合，銀行側はリスクがあると判断し，秘密の質問など，追加認証を行うといった仕組みである。

問7 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，認証局から発行される。公開鍵証明書の検証時の公開鍵証明書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なわれ，公開鍵証明書のシリアル番号がCRLに記載される。

ア：CRLは常に参照される。
イ：ディジタル証明書の有効期限内に失効したものを登録する。
ウ：有効期限内に失効したリストであるため，有効期限が切れるまで失効リストに登録される。

問8 ア

解説 **CRYPTREC**（Cryptography Research and Evaluation Committees）は，電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。公募された暗号技術や，一般的に広く利用されている暗号技術を評価，検討し，安全性や実装性能がともに優れたものを選択する役割がある。

イ：**内閣サイバーセキュリティセンター**（NISC：National center of Incident readiness and Strategy for Cybersecurity）の活動内容である。
ウ：**一般財団法人日本情報経済社会推進協会**（JPDEC：Japan Institute for Promotion of Digital Economy and Community）の活動内容である。
エ：**独立行政法人情報処理推進機構**（IPA：Information-technology Promotion Agency, Japan）による，暗号モジュール試験及び認証制度（JCMVP：Japan Cryptographic Module Validation Program）の活動内容である。

問 9

正解 □ 完璧 □ 直前チェック □

Cookieにsecure属性を付けなかったときと比較した，付けたときの動作の差はどれか。

ア　Cookieに指定された有効期間を過ぎると，Cookieが無効化される。
イ　JavaScriptによるCookieの読出しが禁止される。
ウ　URLのスキームがhttpsのページのときだけ，WebブラウザからCookieが送出される。
エ　WebブラウザがアクセスするURL内のパスとCookieによって指定されたパスのプレフィックスが一致するとき，WebブラウザからCookieが送出される。

問 10

正解 □ 完璧 □ 直前チェック □

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 11

正解 □ 完璧 □ 直前チェック □

マルウェアの活動傾向などを把握するための観測用センサが配備され，ダークネットともいわれるものはどれか。

ア　インターネット上で到達可能，かつ，未使用のIPアドレス空間
イ　組織に割り当てられているIPアドレスのうち，コンピュータで使用されているIPアドレス空間
ウ　通信事業者が他の通信事業者などに貸し出す光ファイバ設備
エ　マルウェアに狙われた制御システムのネットワーク

問9　ウ

解説　Cookieのsecure属性は，https通信の場合のみ，Webブラウザから送出される。httpの場合は，暗号化されていない通信であるため，Cookieの盗聴リスクがある。

問10　ア

解説　**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暗号を直接解読するのではなく，発生する電磁波，熱，演算処理時間などの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11　ア

解説　**ダークネット**とは，インターネット上の未使用のIPアドレス空間のことを示す。
ダークネットに到来するパケットを観測することで，インターネットを経由して感染を広めるマルウェアの活動傾向などを把握することができる。

問 12 正解 完璧 直前チェック

rootkitの特徴はどれか。

ア　OSなどに不正に組み込んだツールを隠蔽する。
イ　OSの中核であるカーネル部分の脆弱性を分析する。
ウ　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。
エ　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。

問 13 正解 完璧 直前チェック

DNSSECで実現できることはどれか。

ア　DNSキャッシュサーバが得た応答中のリソースレコードが，権威DNSサーバで管理されているものであり，改ざんされていないことの検証
イ　権威DNSサーバとDNSキャッシュサーバとの通信を暗号化することによる，ゾーン情報の漏えいの防止
ウ　長音“ー”と漢数字“一”などの似た文字をドメイン名に用いて，正規サイトのように見せかける攻撃の防止
エ　利用者のURLの打ち間違いを悪用して，偽サイトに誘導する攻撃の検知

問 14 正解 完璧 直前チェック

IEEE 802.1Xで使われるEAP-TLSによって実現される認証はどれか。

ア　CHAPを用いたチャレンジレスポンスによる利用者認証
イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証
ウ　ディジタル証明書による認証サーバとクライアントの相互認証
エ　利用者IDとパスワードによる利用者認証

問12　ア

解説 **rootkit**とは，クラッカがセキュリティホール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，踏み台による攻撃などに用いる機能をまとめたツール群のことである。

イ：**セキュリティツール**の説明である。セキュリティツールはカーネルの脆弱性以外にも，多種多様なソフトウェアを解析するためのツールの総称である。

ウ：**ウイルス対策ソフト**の説明である。

エ：**ポートスキャンツール**の説明である。

問13　ア

解説 **DNSSEC**（Domain Name System Security Extension）：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証明するセキュリティ拡張機能のことである。応答を送信するDNSサーバが秘密鍵を使って応答に署名し，受信する側が公開鍵で検証する。秘密鍵で正しい署名を付けるので，署名の検証によって偽の応答を検知できる。

問14　ウ

解説 **IEEE 802.1X**は，クライアントPCと，無線のアクセスポイントやスイッチングハブとの間で利用される，ディジタル証明書による認証プロトコルである。鍵交換により共有された鍵を用いて，クライアントPCと接続先との暗号化通信を行う。

IEEE 802.1Xでは，**EAP-TLS**や**EAP-PEAP**などの認証方式が使用される。

EAP-TLS（Extensible Authentication Protocol - Transport Layer Security）：EAPは，サーバとクライアント間の認証プロトコルである。TLSは，電子証明書を利用して認証を行う方式である。

EAP-PEAP（Extensible Authentication Protocol - Protected Extensible Authentication Protocol）：EAPは，サーバとクライアント間の認証プロトコルである。PEAPは，パスワード入力によって認証を行う方式である。

問 15 正解 完璧 直前チェック

IPsecに関する記述のうち，適切なものはどれか。

ア　IKEはIPsecの鍵交換のためのプロトコルであり，ポート番号80が使用される。
イ　暗号化アルゴリズムとして，HMAC-SHA1が使用される。
ウ　トンネルモードを使用すると，暗号化通信の区間において，エンドツーエンドの通信で用いる元のIPのヘッダを含めて暗号化できる。
エ　ホストAとホストBとの間でIPsecによる通信を行う場合，認証や暗号化アルゴリズムを両者で決めるためにESPヘッダではなくAHヘッダを使用する。

問 16 正解 完璧 直前チェック

SMTP-AUTHの特徴はどれか。

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接続を禁止する。
イ　電子メール送信元のサーバが，送信元ドメインのDNSに登録されていることを確認して，電子メールを受信する。
ウ　メールクライアントからメールサーバへの電子メール送信時に，ユーザアカウントとパスワードによる利用者認証を行う。
エ　メールクライアントからメールサーバへの電子メール送信は，POP接続で利用者認証済みの場合にだけ許可する。

問15　ウ

解説 **IPsec**は，インターネットで暗号通信を行うための規格である。IPv6では標準で実装されている。

ア：UDPポート番号500が使用される。
イ：IPsecでは鍵交換プロトコルとしてIKE（Internet Key Exchange）が使用される。**HMAC-SHA1**は，IPsecのAHヘッダ（認証ヘッダ）などの認証機構に採用されている鍵ハッシュ関数を利用したメッセージ認証方式である。
ウ：IPsecの通信モードには，データ部分のみを認証/暗号化して元のIPヘッダは対象としない**トランスポートモード**と，IPヘッダも含めて暗号化・カプセル化する**トンネルモード**の二つがある。トランスポートモードはエンドツーエンドで認証や暗号化を行う場合に使用し，トンネルモードはネットワーク間の通信に対して認証や暗号化を行う場合に使用される。よって正解となる。
エ：**AHヘッダ**では暗号化はできない。

問16　ウ

解説 **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だけ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：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の対策である。
エ：**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が開発された当初は，ユーザ認証機能が実装されていなかったため，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。

問 17 正解 完璧 直前チェック

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サーバを稼働させる。
イ	セッションIDを乱数で生成する。	TLSによって通信内容を秘匿する。
ウ	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。
エ	プレースホルダを利用する。	データベースのアカウントがもつデータベースアクセス権限を必要最小限にする。

問 18 正解 完璧 直前チェック

DNSに関する記述のうち，適切なものはどれか。

ア　DNSサーバに対して，IPアドレスに対応するドメイン名，又はドメイン名に対応するIPアドレスを問い合わせるクライアントソフトウェアを，リゾルバという。

イ　問合せを受けたDNSサーバが要求されたデータをもっていない場合に，他のDNSサーバを参照先として回答することを，ゾーン転送という。

ウ　ドメイン名に対応するIPアドレスを求めることを，逆引きという。

エ　ドメイン名を管理するDNSサーバを指定する資源レコードのことを，CNAMEという。

問17　エ

解説 **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にする攻撃のことである。対策としては，**プレースホルダ**を利用する。プレースホルダは，「$1」や「?」のように，SQL文の中で入力された文字列を他の文字列に置換・代替する変数である。

また，データベースのアカウントのも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18　ア

解説 **DNS**（**Domain Name System**）は，TCP/IPネットワークで用いられるネームサービスの仕組みのことで，ドメイン名やホスト名とIPアドレスの対応表を使って，ホスト名とIPアドレスを互いに変換する機能をもつ。DNSサーバに対して，IPアドレスに対応するドメイン名，又はドメイン名に対応するIPアドレスを問い合わせるクライアントソフトウェアを，**リゾルバ**という。

イ：他のDNSサーバを参照先として回答することを，**フォワーダ**という。

ウ：ドメイン名に対するIPアドレスを求めることは，**正引き**という。

エ：資源レコードは，**リソースレコード**（**RR**：Resource Record）という。

主なリソースレコードと役割は以下の通り。

MX（Mail eXchanger）レコード：電子メールの送信に利用される。

CNAME（Canonical Name）レコード：ホスト名に別名をつけるために利用される。

A（Address）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に利用される。

PTR（PoinTeR）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に利用される。

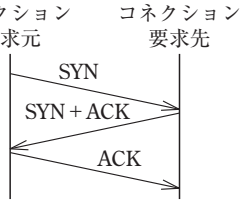
NS（Name Server）レコード：ドメイン名の委任を行うことに利用される。NSレコードを持ったサーバはドメインに対する正式なサーバとみなされる。

SOA（Start Of Authority）レコード：ドメイン名のレコードの基本情報を示すために利用される。

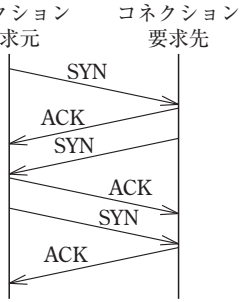
問 19 正解 完璧 直前チェック

TCPのコネクション確立方式である3ウェイハンドシェイクを表す図はどれか。

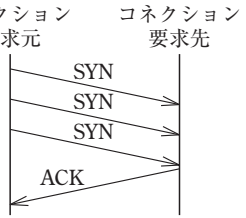
ア



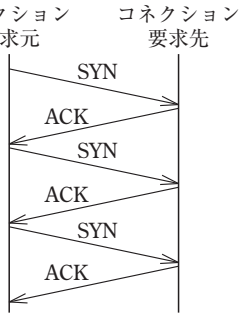
イ



ウ



エ



問 20 正解 完璧 直前チェック

TCPに関する記述のうち，適切なものはどれか。

ア　OSI基本参照モデルのネットワーク層の機能である。
イ　ウィンドウ制御の単位は，バイトではなくビットである。
ウ　確認応答がない場合は再送処理によってデータ回復を行う。
エ　データの順序番号をもたないので，データは受信した順番のままで処理する。

問19　ア

解説 **TCP**は，通信のコネクションの要求元と要求先で相互の状況を確認してからデータを送り，データの到着を確認してから次のデータを送るというコネクション確立方式の通信を行う。要求元は要求先に**SYN**（SYNchronization：同期）を送信する。要求先はそれを受けて，要求を受付けた**ACK**（ACKnowledgement：確認応答）とSYNを返信する。それを受けて要求元はACKを送る。この送信準備を3ウェイハンドシェイクという。要求先の確認を取ることをネゴシエーションという。

ちなみに，**UDP**はコネクションレス方式であるので，送信元は送信先へ直ちにデータを送信する。UDPには再送機能やフロー制御機能はない。

問20　ウ

解説 **TCP**（Transmission Control Protocol）：トランスポート層のプロトコル。コネクションを行うストリーム通信であり，確認応答や順序制御の機能をもつ。

ア：**トランスポート層**のプロトコルである。
イ：**ウインドウ制御**の単位は，バイトである。ウインドウ制御とは，TCPの通信先ホストからの応答（ACK）を待たずに，一度に送信できるデータ制御を指す。
エ：データの順序番号（**シーケンス番号**）をもち，順番が入れ替わっても順序通りにパケットを組み立てる。データの順序番号をもたないのは，UDPである。

問 21 正解 完璧 直前チェック

システム障害発生時には，データベースの整合性を保ち，かつ，最新のデータベース状態に復旧する必要がある。このために，DBMSがトランザクションのコミット処理を完了とするタイミングとして，適切なものはどれか。

ア　アプリケーションの更新命令完了時点
イ　チェックポイント処理完了時点
ウ　ログバッファへのコミット情報書込み完了時点
エ　ログファイルへのコミット情報書込み完了時点

問 22 正解 完璧 直前チェック

システム開発で行うテストについて，テスト要求事項を定義するアクティビティと対応する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21　エ

解説　システム障害が発生した際には，更新前ジャーナルや更新後ジャーナルなどのログファイルを使用して復旧にあたる。したがって，ログファイルへの書出しが完了した時点でコミット処理の完了とみなす。

ア：実更新だけではコミットされていない。
イ：チェックポイント処理とは，あるタイミングでデータベース全体の状態を記録することであるから，本問には不適切である。
ウ：ログバッファへの書込みが完了しても，ログファイルへの書出しまでに障害が発生すると，ログファイルが完成しない。

問22　ウ

解説　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の動作を確認するテスト。
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 正解 完璧 直前チェック

表はシステムの特性や制約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。

開発方針	開発モデル
最初にコア部分を開発し，順次機能を追加していく。	a
要求が明確なので，全機能を一斉に開発する。	b
要求に不明確な部分があるので，開発を繰り返しながら徐々に要求内容を洗練していく。	c

	a	b	c
ア	進化的モデル	ウォータフォールモデル	段階的モデル
イ	段階的モデル	ウォータフォールモデル	進化的モデル
ウ	ウォータフォールモデル	進化的モデル	段階的モデル
エ	進化的モデル	段階的モデル	ウォータフォールモデル

問 24 正解 完璧 直前チェック

JIS Q 20000-1で定義されるインシデントに該当するものはどれか。

ア　ITサービス応答時間の大幅な超過
イ　ITサービスの新人向け教育の依頼
ウ　ITサービスやシステムの機能，使い方に対する問合せ
エ　新設営業所に対するITサービス提供の要求

問23　イ

解説

段階的モデル：開発要求を取り入れながら，開発する範囲に順序付けを行う。順序に従って部分的に分けて開発する手法。
ウォータフォールモデル：システム開発における各工程を順番に進めていく開発手法。
進化的モデル：部分的に定義された要求から開発を開始し，後続の開発で要求を適用することで真の要求に近づけていく開発手法。

問24　ア

解説 **JIS Q 20000-1**は，ISO/IEC 20000-1を基に作成された日本工業規格である。**ITIL**（Information Technology Infrastructure Library）と同意語となるプロセスによって定義されている。**インシデント**とは，正常に稼動しているサービスを阻害するイベントや状態をいう。

ア：システムの可用性に影響がある状態といえるため，インシデントとなる。
イ，ウ，エ：依頼，問合せ，要求は，サービスを阻害する要因ではないため，インシデントではない。

問 25

正解 □ 完璧 □ 直前チェック □

データベースに対する不正アクセスの防止・発見を目的としたアクセスコントロールについて，“システム管理基準”への準拠性を確認する監査手続として，適切なものはどれか。

ア　利用者がデータベースにアクセスすることによって業務が効率的に実施できるかどうかを確認するために，システム仕様書を閲覧する。

イ　利用者がデータベースにアクセスするための画面の操作手順が操作ミスを起こしにくい設計になっているかどうかを確認するために，利用者にヒアリングする。

ウ　利用者が要求した応答時間が実現できているかどうかを確認するために，データベースにアクセスしてから出力結果が表示されるまでの時間を測定する。

エ　利用者のデータベースに対するアクセス状況を確認するために，アクセス記録を出力し内容を調査する。

問25　エ

解説　**システム管理基準**：組織が主体的に経営戦略に沿って効果的な情報システム戦略を立案し，その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で，効果的な情報システム投資のための，リスクを低減するためのコントロールを適切に整備・運用するための実践規範。

データベースに対する不正アクセスの防止・発見を目的としたアクセスコントロールではアクセスの記録内容の監査を行うことが有効である。アクセスログから，いつだれがアクセスしたかを監査する。

ア：効率的に業務ができること確認は，不正アクセスの防止・発見を目的とした監査ではない。

イ：操作ミス防止の確認は，不正アクセスの防止・発見を目的とした監査ではない。

ウ：応答性能の確認は，不正アクセスの防止・発見を目的とした監査ではない。