問題

問 1

正解 完璧 直前CHECK

APT（Advanced Persistent Threats）の説明はどれか.

ア　攻撃者はDoS攻撃及びDDoS攻撃を繰り返し組み合わせて，長期間にわたって特定組織の業務を妨害する.

イ　攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す.

ウ　攻撃者は特定の目的をもち，特定組織を標的に複数の手法を組み合わせて気付かれないよう執拗に攻撃を繰り返す.

エ　攻撃者は不特定多数への感染を目的として，複数の攻撃方法を組み合わせたマルウェアを継続的にばらまく.

問 2

正解 完璧 直前CHECK

DNSSEC（DNS Security Extensions）の機能はどれか.

ア　DNSキャッシュサーバの設定によって再帰的な問合せの受付範囲が最大になるようにする.

イ　DNSサーバから受け取るリソースレコードに対するディジタル署名を利用して，リソースレコードの送信者の正当性とデータの完全性を検証する.

ウ　ISPなどのセカンダリDNSサーバを利用してDNSコンテンツサーバを二重化することで名前解決の可用性を高める.

エ　共通鍵暗号技術とハッシュ関数を利用したセキュアな方法で，DNS更新要求が許可されているエンドポイントを特定し認証する.

問 3

正解 完璧 直前CHECK

PKIを構成するOCSP（Online Certificate Status Protocol）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　有効期限の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1　ウ

APT（標的型諜報攻撃）の一番の特徴は，特定組織を標的とした目的を持った攻撃である．攻撃手法は，攻撃対象者へメールでウイルスを送付し，ウイルスを実行させることでバックドアを開通し，リモートコントロールによる情報の搾取である．APTは，複数の攻撃を組み合わせることや特定システムへの継続的なハッキングなど複雑であるため，危険かつ対策が困難な攻撃である．

ア：複数の手法を組み合わせて高度化されていない攻撃はAPTとはならない．

イ，エ：攻撃対象を特定しない場合は，APTとはならない．

問2　イ

DNSSEC（DNS Security Extensions）：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．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．そのためDNSキャッシュポイズニングを防ぐことができる．

ア：再帰的な問い合わせの受付範囲を最大限にすると，DDoS攻撃の踏み台にされる危険性がある．

ウ：DNSは一般的に，プライマリサーバと，セカンダリサーバを用意し，2台以上で情報を管理する．内容は正しいが，DNSSECの内容ではない．

エ：DNSSECは，公開鍵を利用するため，共通鍵暗号技術という説明は誤っている．

問3　ウ

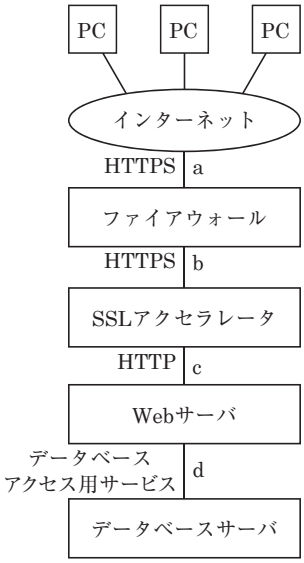
OCSP（Online Certificate Status Protocol）は，ディジタル証明書の失効情報をリアルタイムで確認するためのプロトコルである．OCSPはCRL（証明書失効リスト）の代替として策定され，CRLを持たなくてもリアルタイムで失効情報を確認することが可能である．RFC2560によって規定されている．

問題

問 4

正解 □ 完璧 □ 直前CHECK □

図のような構成と通信サービスのシステムにおいて，Webアプリケーションの脆弱性対策としてネットワークのパケットをキャプチャしてWAFによる検査を行うとき，WAFの設置場所として最も適切な箇所はどこか．ここで，WAFには通信を暗号化したり，復号したりする機能はないものとする．



ア　a　　イ　b　　ウ　c　　エ　d

問 5

正解 □ 完璧 □ 直前CHECK □

サイドチャネル攻撃の説明はどれか．

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量（処理時間や消費電流など）やエラーメッセージから，攻撃対象の機密情報を得る．

イ　企業などの機密情報を詐取するソーシャルエンジニアリングの手法の一つであり，オフィスの紙ゴミの中から不用意に捨てられた機密情報の印刷物を探し出す．

ウ　通信を行う二者の間に割り込んで，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，気付かれることなく盗聴する．

エ　データベースを利用するWebサイトに入力パラメタとしてSQL文の断片を与えることによって，データベースを改ざんする．

問4　ウ

WAF（Web Application Firewall）は，Webアクセスの内容を把握し，不正侵入を検知・防御するシステムである．一般的にFirewallは，TCPやUDPといったプロトコルとポート番号といったOSI基本参照モデルのトランスポート層での防御であるがWAFは，OSI基本参照モデルのアプリケーション層での防御となる．

WAFは，HTTP通信の内容を識別する必要があるため，HTTPSでの暗号化が復号され，HTTPでの通信となる位置に設置する．

問5　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．

イ：スキャベジングの説明である．

ウ：**中間者攻撃**（man in the middle attack）の説明である．

エ：**SQLインジェクション攻撃**の説明である．

問 6

正解 □ 完璧 □ 直前CHECK □

SMTP-AUTHにおける認証の動作を説明したものはどれか.

ア　SMTPサーバに電子メールを送信する前に，電子メールを受信し，その際にパスワード認証が行われたクライアントのIPアドレスは，一定時間だけ電子メールの送信が許可される.

イ　クライアントがSMTPサーバにアクセスしたときに利用者認証を行い，許可された利用者だけから電子メールを受け付ける.

ウ　サーバは認証局のディジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する.

エ　利用者が電子メールを受信する際の認証情報を秘匿できるように，パスワードからハッシュ値を計算して，その値で利用者認証を行う.

問 7

正解 □ 完璧 □ 直前CHECK □

無線LAN環境に複数台のPC，複数のアクセスポイント及び利用者認証情報を管理する1台のサーバがある．利用者認証とアクセス制御にIEEE 802.1XとRADIUSを利用する場合の実装方法はどれか.

ア　PCにはIEEE 802.1Xのサプリカントを実装し，RADIUSクライアントの機能をもたせる.

イ　アクセスポイントにはIEEE 802.1Xのオーセンティケータを実装し，RADIUSクライアントの機能をもたせる.

ウ　アクセスポイントにはIEEE 802.1Xのサプリカントを実装し，RADIUSサーバの機能をもたせる.

エ　サーバにはIEEE 802.1Xのオーセンティケータを実装し，RADIUSサーバの機能をもたせる.

問 8

正解 □ 完璧 □ 直前CHECK □

CSIRTの説明として，適切なものはどれか.

ア　IPアドレスの割当て方針の決定，DNSルートサーバの運用監視，DNS管理に関する調整などを世界規模で行う組織である.

イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である.

ウ　国レベルや企業・組織内に設置され，コンピュータセキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である.

エ　情報技術を利用し，信教や政治的な目標を達成するという目的をもった人や組織の総称である.

問6　イ

SMTP-AUTH認証は，クライアントがメールを送信する際の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電子メールの送信を許可する認証方式である．

SMTP自体は標準で認証する仕様となっておらず，他の方式をあわせて利用制限を行っている．SMTPサーバではIPアドレスや，ドメイン名でアクセスを制限することが一般的であったが，スパムメールに利用されることなどを避けるために，SMTP-AUTHを利用し個人単位でメールを送信する機能が作られた．

ア：POP Before SMTPの認証の説明である．

ウ：SMTP over SSLの説明である．

エ：APOP（Authenticated Post Office Protocol）の説明である．

問7　イ

RADIUS（Remote Authentication Dial In User Service）は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である．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．無線LANだけでなく，優先LANでも利用できる．

IEEE802.1Xでは，認証のためのデータのやりとりを，PCとアクセスポイントで行う．また，アクセスポイントとRADIUSサーバの間ではRADIUSプロトコルによって中継する．

サプリカントとは，IEEE802.1X通信を可能とするためのPC用のソフトウェアである．

ア：PCでは認証自体を行わないため，RADIUSクライアントの機能を持たせない．

イ：正しい．アクセスポイントではRADIUSクライアントの機能を持たせ認証を行う．

ウ：アクセスポイントにはサプリカントを実装しない．

エ：オーセンティケータは，認証を中継するアクセスポイントに持たせる．

問8　ウ

CSIRT（Computer Security Incident Response Team：コンピュータ・セキュリティ・インシデント・レスポンス・チーム）は，セキュリティに関する様々な事象について活動を行う組織の総称である．企業の場合では，CSIRTを立ち上げることで，事象（インシデント）の問い合わせ窓口の設置や，セキュリティ教育，技術情報の提供などを実施することでセキュリティ対応を継続的に高度に対応していくことが可能となる．

問題

問 9

正解 完璧 直前CHECK

NISTの定義によるクラウドコンピューティングのサービスモデルにおいて，パブリッククラウドサービスの利用企業のシステム管理者が，仮想サーバのゲストOSに係る設定作業及びセキュリティパッチ管理作業を実施可かどうかの組合せのうち，適切なものはどれか.

	IaaS	PaaS	SaaS
ア	実施可	実施可	実施不可
イ	実施可	実施不可	実施不可
ウ	実施不可	実施可	実施不可
エ	実施不可	実施不可	実施可

問 10

正解 完璧 直前CHECK

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IT製品のセキュリティ脆弱性の深刻さを評価するものはどれか.

ア CVSS　　イ ISMS　　ウ PCI DSS　　エ PMS

問9　イ

NIST（National Institute of Standards and Technology：**米国国立標準研究所**）は，連邦政府機関の標準およびガイドラインを作成する機関である．

NISTによるパブリッククラウドのサービスモデル定義では，次のように説明されている．

SaaS（Cloud Software as a Service）：利用者に提供される機能は，クラウドのインフラ上で稼動しているプロバイダ由来のアプリケーション．例外はユーザ固有のアプリケーション設定である．

PaaS（Cloud Platform as a Service）：利用者に提供される機能は，クラウドのインフラ上にユーザが開発したまたは購入したアプリケーションを実装することである．サーバ，OS，ストレージの管理権限は利用者に提供されない．

IaaS（Cloud Infrastructure as a Service）：利用者に提供される機能は，演算機能，ストレージ，ネットワークその他の基本的コンピューティングリソースである．利用者は任意のソフトゥエアを実装し走らせることができる．

本問では，OSに係る設定作業とセキュリティパッチ管理作業を利用者企業の管理であるか，サービス提供側であるかとなるため，イの範囲が正しいとなる．

問10　ア

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（Base Metrics），現状評価基準（Temporal Metrics），環境評価基準（Environmental Metrics）といった三つの基準で脆弱性を評価する．

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．

ISMS（Information Security Management System）：情報セキュリティマネジメントシステム）とは，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．計画（Plan），実行（Do），確認（Check），改善（Action）の各フェーズを繰り返しながら，セキュリティレベルを改善していく．

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）：日本語では個人情報保護マネジメントシステムのことで，プライバシーマーク（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．

問題

問 11

正解 □ 完璧 □ 直前CHECK □

CRYPTRECの活動内容はどれか.

ア　客観的な評価によって安全性及び実装性に優れると判断された暗号技術のリストを決定する.

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.

問 12

正解 □ 完璧 □ 直前CHECK □

企業のDMZ上で1台のDNSサーバをインターネット公開用と社内用で共用している．このDNSサーバが，DNSキャッシュポイズニングの被害を受けた結果，直接引き起こされ得る現象はどれか.

ア　DNSサーバのハードディスク上のファイルに定義されたDNSサーバ名が書き換わり，外部からの参照者が，DNSサーバに接続できなくなる.

イ　DNSサーバのメモリ上にワームが常駐し，DNS参照元に対して不正プログラムを送り込む.

ウ　社内の利用者が，インターネット上の特定のWebサーバを参照しようとすると，本来とは異なるWebサーバに誘導される.

エ　社内の利用者間で送信された電子メールの宛先アドレスが書き換えられ，正常な送受信ができなくなる.

問 13

正解 □ 完璧 □ 直前CHECK □

ウイルスの検出手法であるビヘイビア法を説明したものはどれか.

ア　あらかじめ特徴的なコードをパターンとして登録したウイルス定義ファイルを用いてウイルス検査対象と比較し，同じパターンがあれば感染を検出する.

イ　ウイルスに感染していないことを保証する情報をあらかじめ検査対象に付加しておき，検査時に不整合があれば感染を検出する.

ウ　ウイルスの感染が疑わしい検査対象を，安全な場所に保管されている原本と比較し，異なっていれば感染を検出する.

エ　ウイルスの感染や発病によって生じるデータ書込み動作の異常や通信量の異常増加などの変化を監視して，感染を検出する.

問11　ア

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，安全性や実装性能ともに優れたものを選択する役割がある．

問12　ウ

DNSキャッシュポイズニングとは，URLといったDNSを利用したIPアドレス検索を行う際に正しいIPアドレスを検索できなくすること．攻撃者が不正なIPアドレスを返すようDNSのキャッシュ（一定期間IPアドレス情報を記憶している仕組み）を汚染させることである．そのため，汚染されたキャッシュ上のWebサーバにアクセスしようとすると本来とは異なるサーバに誘導される．

問13　エ

ビヘイビア法は，ウイルスの感染や発病による異常な振る舞い（システム領域の書込み動作や，通信量の増加等）を監視し，ウイルスを検出する手法である．ビヘイビア法の特徴としては，システム上の異常な振る舞いを監視しているため，既存のウイルスの亜種や未知のウイルスであっても検出できることがある．

ア：パターンマッチング法の説明である．

イ：チェックサム法の説明である．

ウ：コンペア法の説明である．

問 14

正解 □ 完璧 □ 直前CHECK □

DoS攻撃の一つであるSmurf攻撃の特徴はどれか.

ア　ICMPの応答パケットを大量に発生させる.
イ　TCP接続要求であるSYNパケットを大量に送信する.
ウ　サイズが大きいUDPパケットを大量に送信する.
エ　サイズが大きい電子メールや大量の電子メールを送信する.

問 15

正解 □ 完璧 □ 直前CHECK □

ダウンローダ型ウイルスが内部ネットワークのPCに感染した場合に，インターネット経由で他のウイルスがダウンロードされることを防ぐ対策として，最も有効なものはどれか.

ア　URLフィルタを用いてインターネット上の不正Webサイトへの接続を遮断する.
イ　インターネットから内部ネットワークに向けた要求パケットによる不正侵入行為をIPSで破棄する.
ウ　スパムメール対策サーバでインターネットからのスパムメールを拒否する.
エ　メールフィルタで他サイトへの不正メール発信を遮断する.

問 16

正解 □ 完璧 □ 直前CHECK □

スパムメールの対策であるDKIM（DomainKeys Identified Mail）の説明はどれか.

ア　送信側メールサーバでディジタル署名を電子メールのヘッダに付加して，受信側メールサーバで検証する.
イ　送信側メールサーバで利用者が認証されたとき，電子メールの送信が許可される.
ウ　電子メールのヘッダや配送経路の情報から得られる送信元情報を用いて，メール送信元のIPアドレスを検証する.
エ　ネットワーク機器で，内部ネットワークから外部のメールサーバのTCPポート番号25への直接の通信を禁止する.

問14　ア

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．攻撃の手法は次のとおり．

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装して，Echo Requestをブロードキャストアドレス宛に送信する．Echo Replyがネットワークの全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．

イ：**SYN flood攻撃**の説明である．

ウ：**UDP flood攻撃**の説明である．

エ：**メール爆弾**（Mail Bomb）**攻撃**の説明である．

問15　ア

ダウンローダ型ウイルスとはトロイの木馬型ウイルスの一種で，コンピュータのOSやアプリケーションソフトの脆弱性を利用して感染した後，別のPCへの感染活動だけでなく，別のウイルスをインターネットからダウンロードするという特徴がある．

ア：正しい．ダウンロード先の不正Webサイトの URLが判明している場合，URLフィルタを用いて不正Webサイトへの接続を遮断する．

イ：ダウンローダ型ウイルスは内部ネットワークから外部ネットワークであるインターネットへアクセスするため，IPSはウイルスのダウンロード防止の効果はない．

ウ：スパムメールの中にはウイルスが添付されていたり，ウイルスをダウンロードさせるWebサイトへ誘導したりするものもある．ダウンローダ型ウイルスの感染予防にはなる．

エ：不正メールの発信防止であり，ダウンローダ型ウイルスの対策とは無関係である．

問16　ア

DKIMは，送信者が正当な団体であるかどうかを認証する送信者認証技術である．メールを送信するときに自分が持っている秘密鍵でディジタル署名を行い，メールを受け取る受信側では送信情報を元にDNSを管理しているサーバに問い合わせて公開鍵を取得する．

イ：SMTP-AUTHの説明である．

ウ：ブラックリストの説明である．スパムメール送信元IPアドレスのブラックリストを照合する．

エ：OP25Bの説明である．

問題

問 17

正解 完璧 直前CHECK

IEEE 802.11aやIEEE 802.11bで採用されているアクセス制御方式はどれか.

ア　CSMA/CA
イ　CSMA/CD
ウ　LAPB
エ　トークンパッシング方式

問 18

正解 完璧 直前CHECK

IPv6グローバルユニキャストアドレスはどれか.

ア　::1
イ　2001:dc3::35
ウ　fd00::12:fff:fea9:18
エ　fe80::f:acff:fea9:18

問 19

正解 完璧 直前CHECK

TCPのフロー制御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 17　ア

CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance）：パケットを送信する際に一定時間以上回線が空いていることを確認してから送信を開始する．衝突を検出できない無線LANなどの場合に用いる．

CSMA/CD（Carrier Sense Multiple Access with Collision Detection）：CSMA/CAと異なり，パケットを送信する際に衝突を検出することができる．衝突を検出した場合は，しばらく待ってから再送信を行う．

LAPB（Link Access Procedure Balanced）：平衡型リンクアクセス手順．X.25やISDNのBチャネル用データリンク層プロトコルである．パケット交換網などで利用される．

トークンパッシング方式：パケットを送信する際にトークンと呼ばれる送信権のデータがつながっている端末を巡回し，トークンが届いた場合のみ端末はデータを伝送できる．

問 18　イ

IPv6のIPアドレス長は，128ビットとなっている．表記方法は，16ビット単位に：（コロン）で区切る形である．RFC5952では表記ルールの0の省略方法を示している．

1. 16ビットの“：”区切りの先頭にある0は省略
   例　2001:0dc3:: = 2001:dc3::
2. 0000が連続する場合 :: を使用して可能な限り省略
3. 0000が1箇所しかない場合 :: を使用して省略してはならない
4. “::”を使用して使用して省略可能な箇所が複数ある場合は，もっとも多く0を省略できる箇所を省略．ただし複数個所で0の数が同じ場合は先の0を省略

アドレスのフォーマットは次のようになる．

選択肢	アドレスの型	IPv6 表記
ア	ループバックアドレス	::1/128
イ	グローバルユニキャストアドレス	上記以外
ウ	ユニークローカルユニキャスト	fe00::/7
エ	リンクローカルユニキャストアドレス	fe80::/10
–	マルチキャストアドレス	ff00::/8

/7や，/8 のスラッシュ表記は，先頭から7ビット，8ビット部分がサブネット番号を指す．

問 19　ウ

フロー制御とは，受信側の端末でパケットを受け取りきれなくなるとき，送信を一時的に停止または送出速度を落とすことを送信側に要請し，受信量を調整する仕組みである．ウィンドウサイズが大きくなると，受信確認をせずに多くのパケットを送信できるため，パフォーマンスが良くなる．

ア：TCPはトランスポート層（4層）の機能である．

イ：ウィンドウ制御はセグメント単位で行う．

エ：シーケンス番号という順序番号を持ち順序制御がある．

問 20

正解 □ 完璧 □ 直前CHECK □

電子メールが配送される途中に経由したMTAのIPアドレスや時刻などの経由情報を，MTAが付加するヘッダフィールドはどれか.

ア　Accept　　イ　Received　　ウ　Return-Path　　エ　Via

問 21

正解 □ 完璧 □ 直前CHECK □

関係データベースのビューを利用する目的はどれか.

ア　DISTINCT指定，GROUP BY句及びHAVING句をもつ演算処理を独立させて，プログラムに単純化したデータ更新手段を提供する.

イ　行や列を特定の条件で絞り込んだビューだけをアクセスさせることによって，基となる表のデータの一部を隠蔽して保護する手段を提供する.

ウ　データベースの物理的記憶構造の変更に影響されないように，アプリケーションプログラムに対して物理的データ独立性を提供する.

エ　複数の表を結合したビューにインデックスを付与することによって，複数の表にまたがった高度な検索手段を提供する.

問 22

正解 □ 完璧 □ 直前CHECK □

既存システムを基に，新システムのモデル化を行う場合のDFD作成の手順として，適切なものはどれか.

ア　現物理モデル → 現論理モデル → 新物理モデル → 新論理モデル

イ　現物理モデル → 現論理モデル → 新論理モデル → 新物理モデル

ウ　現論理モデル → 現物理モデル → 新物理モデル → 新論理モデル

エ　現論理モデル → 現物理モデル → 新論理モデル → 新物理モデル

問20　イ

MTA（Mail Transfer Agent）は，電子メールを相手に送信するためのメールサーバで起動するソフトウェアである．メールを配送する際にMTAは，メールヘッダに対して送信元や経由，時間などの配送情報を負荷する．郵便に例えると消印と考えればよい．Receivedヘッダは次のとおりとなる．

Received:from< 送信サーバ >by< 受信サーバ >via< 接続方式 >with< 転送方式 >id< 識別番号 >for< 宛先 >;< 受信日時 >

問21　イ

ビュー（仮想の表）は，関係データベースの操作言語であるSQLによって，一つ以上の表（ビュー）から任意のデータ選択し表すものである．

ビューを生成することで，複数の表に点在するデータを一つの表に仮想的にまとめることにより，処理や操作が容易になる．また，利用者の権限に応じてアクセスできるデータをビューによって管理することができるためセキュリティが向上する．

問22　イ

DFDは，現物理モデル，現論理モデル，新論理モデル，新物理モデルの四つのモデルを作成する．DFD作成の手順は，次のような流れになる．

【要求定義・分析】

現物理モデル：今の業務をありのままに記述する．例えば伝票に手書きする，請求書を書くなどである．

現論理モデル：現物理モデルから人間的な部分を排除したものである．例えば入力する，出力するなど，機能に注目して作成する．

新論理モデル：システム化する部分について，現論理モデルの問題点の解決や，新たな業務処理の追加を行う．

【外部設計】

新物理モデル：システム化した部分を使って新たな業務の流れを記述したものである．新システムが導入された後の仕事の流れを記述する．

問題

問 23

正解 □ 完璧 □ 直前CHECK □

SOA（Service Oriented Architecture）でサービスを設計する際の注意点のうち，適切なものはどれか．

ア　可用性を高めるために，ステートフルなインタフェースとする．
イ　業務からの独立性を確保するために，サービスの命名は役割を表すものとする．
ウ　業務の変化に対応しやすくするために，サービス間の関係は疎結合にする．
エ　セキュリティを高めるために，一度開発したサービスは再利用しない方がよい．

問 24

正解 □ 完璧 □ 直前CHECK □

情報システムの設計のうち，フェールソフトの例はどれか．

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し，データを保全する．
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CHECK □

新システムへの移行に関するシステム監査で確認した状況のうち，指摘事項に該当するものはどれか．

ア　移行作業と併せて，システム運用部門及びシステム利用部門に対する新システムの操作教育を計画し，実施していた．
イ　移行対象，移行方法，移行実施体制及び移行スケジュールを明記した移行計画に従って，移行作業を行っていた．
ウ　移行ツールを利用して，データベースの移行及びその移行結果の検証を行っていた．
エ　システム開発部門内に検証体制を作って移行結果の検証を行い，移行完了としていた．

問23　ウ

SOA（Service Oriented Architecture）は，大規模なシステムをサービスの集まりとして，システムを構築する考え方である．

個々のサービスの中はブラックボックスとなり，サービス間のインターフェースは共通化かつ，疎結合となる．インターフェースの共通化，疎結合となることで大規模化の影響が小さくなる．

問24　ウ

フェールソフトは，システムの一部が故障しても，システムが停止せずに一部の機能だけでも継続維持していく機能である．冗長化システムで一部故障しても縮退運転によりシステムを継続運転するものなどが該当する．

ア：フォールトトレランスを意味する．

イ：フェールセーフの説明である．

エ：フールプルーフの説明である．

問25　エ

新システムの移行に関する監査では，開発部門，運用部門，利用部門など各部門が，移行結果が正しいか検証を行う必要がある．一つの部門のみで実施した場合は，他部門への影響が出る可能性が高い．