問題

問 1

正解 完璧 直前CHECK

セキュアハッシュ関数SHA-256を用いて，32ビット，256ビット，2,048ビットの三つの長さのメッセージからハッシュ値を求めたとき，それぞれのメッセージのハッシュ値の長さはどれか．

単位 ビット

	メッセージの長さ		
	32	256	2,048
ア	32	256	256
イ	32	256	2,048
ウ	256	256	256
エ	256	256	2,048

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　エンベロービング署名（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

A社のWebサーバは，認証局で生成したWebサーバ用のディジタル証明書を使ってSSL/TLS通信を行っている．PCがA社のWebサーバにSSL/TLSを用いてアクセスしたとき，サーバのディジタル証明書を入手した後に，認証局の公開鍵を利用しPCが行う処理はどれか．

ア　暗号化通信に利用する共通鍵を生成し，認証局の公開鍵を使って暗号化する．
イ　暗号化通信に利用する共通鍵を認証局の公開鍵を使って復号する．
ウ　ディジタル証明書の正当性を認証局の公開鍵を使って検証する．
エ　利用者が入力，送付する秘匿データを認証局の公開鍵を使って暗号化する．

問1　ウ

SHA-256は2002年に米国家安全保障局（NSA）が設計し，NISTが規格化した米国政府標準ハッシュ関数であり，ハッシュ長は256ビットである．SHA-256はメッセージの長短に無関係に256ビットのハッシュ値が求められる．

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　ウ

A社のWebサーバにSSL/TLSを用いてアクセスしたとき，サーバのディジタル署名を入手後，認証局の公開鍵を利用してPCが行う処理は，**ディジタル証明書の正当性を認証局の公開鍵を使って検証すること**である．その後，PC側で乱数を生成して証明書から取り出したサーバの公開鍵で暗号化して，A社のWebサーバへ送信する．PCとWebサーバは乱数を基に共通鍵を生成して，A社とPCは相互に暗号化通信を行う．

問題

問 4

正解 完璧 直前CHECK

S/KEYワンタイムパスワードに関する記述のうち，適切なものはどれか.

ア　クライアントは認証要求のたびに，サーバへシーケンス番号と種（Seed）からなるチャレンジデータを送信する.

イ　サーバはクライアントから送られた使い捨てパスワードを演算し，サーバで記憶している前回の使い捨てパスワードと比較することによって，クライアントを認証する.

ウ　時刻情報を基にパスワードを生成し，クライアント，サーバ間でパスワードを時刻で同期させる.

エ　利用者が設定したパスフレーズは1回ごとに使い捨てる.

問 5

正解 完璧 直前CHECK

100人の送受信者が共通暗号鍵方式で，それぞれ秘密に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 6

正解 完璧 直前CHECK

情報漏えいに関するリスク対応のうち，リスク回避に該当するものはどれか.

ア　外部の者が侵入できないように，入退室をより厳重に管理する.

イ　情報資産を外部のデータセンタに預託する.

ウ　情報の重要性と対策費用を勘案し，あえて対策をとらない.

エ　データの安易な作成を禁止し，不要なデータを消去する.

問4　イ

S/KEYは，米国ベルコア社が開発したワンタイムパスワード認証方式である．カウンタ値を基に，MD4などのハッシュ関数を使ってパスフレーズをカウンタ回数分計算し，ワンタイムパスワードを導き出す．カウンタが異なればハッシュ関数の利用回数が異なり，毎回異なるワンタイムパスワードが計算される仕組みである．

ア：チャレンジレスポンス方式の説明．

ウ：時刻情報を用いるワンタイムパスワード製品はいくかあるが，S/KEYでは時刻情報を用いていない．

エ：S/KEYの説明ではない．ワンタイムパスワードでは，利用者が1回ごとに設定したパスフレーズを使い捨てるというのは運用が困難であるため，使い捨てにしない．

問5　イ

共通鍵暗号方式でn人の送受信者が相互に暗号を使って秘密に通信を行うとき，n人の中のある人が他の$n-1$人と通信するためには$n-1$個の鍵が必要である．n人全体では，$n(n-1)$個の鍵を必要とする．ただし，送信者と受信者で使う鍵は共通なので，全体では$n(n-1)/2$個になる．

100人の場合は，$100(100-1)/2=4{,}950$の鍵が必要である．

問6　エ

情報漏えいとは，内部の機密情報が外部に漏れてしまうことである．大量の情報をコンピュータで保存できるようになったため，情報漏えいのリスクに対応する必要がある．

ア：リスクの低減（軽減）に関する記述である．

イ：リスクの移転に関する記述である．

ウ：リスクの保有に関する記述である．

問題

問 7

正解 □ 完璧 □ 直前CHECK □

経済産業省告示の“ソフトウェア等脆弱性関連情報取扱基準”におけるWebアプリケーションに関する脆弱性関連情報の適切な取扱いはどれか.

ア　Webアプリケーションの脆弱性についての情報を受けた受付機関は，発見者の氏名・連絡先をWebサイト運営者に通知する.

イ　Webアプリケーションの脆弱性についての通知を受けたWebサイト運営者は，当該脆弱性に起因する個人情報の漏えいなどが発生した場合，事実関係を公表しない.

ウ　受付機関は，Webサイト運営者からWebアプリケーションの脆弱性が修正されたという通知を受けたら，それを速やかに発見者に通知する.

エ　受付機関は，一般利用者に不安を与えないために，Webアプリケーションの脆弱性関連情報の届出状況は，受付機関の中で管理し，公表しない.

問 8

正解 □ 完璧 □ 直前CHECK □

DNSサーバに格納されるネットワーク情報のうち，第三者に公開する必要のない情報が攻撃に利用されることを防止するための，プライマリDNSサーバの設定はどれか.

ア　SOAレコードのシリアル番号を更新する.

イ　外部のDNSサーバにリソースレコードがキャッシュされる時間を短く設定する.

ウ　ゾーン転送を許可するDNSサーバを登録する.

エ　ラウンドロビン設定を行う.

問7　ウ

ア：発見者の氏名，連絡先等は通知しない．

ソフトウェア等脆弱性関連情報取扱基準

Ⅵ．対象がウェブアプリケーションである場合の脆弱性関連情報取扱基準

2．受付機関基準

(4) 受付機関は，氏名，連絡先等の発見者を特定し得る情報を適切に管理し，当該発見者の同意がない場合は他者（調整機関及び製品開発者を含む．）に開示しないこと．

イ：個人情報漏えいの事実が公開されないと，それを知らない個人が架空請求などの二次被害を受ける恐れがある．

同　3．ウェブサイト運営者基準

(4) ウェブサイト運営者は，当該脆弱性に起因する個人情報の漏えい等の事案が発生した場合，二次被害の防止，類似事案の発生回避等の観点から，可能な限り事実関係等を公表するなど必要な対策をとること．

ウ：正しい取扱いである．

同　2．受付機関基準

(6) 受付機関は，当該ウェブサイト運営者から当該脆弱性を修正した旨の通知があったときは，それを速やかに発見者に通知すること．

エ：Webアプリケーションの脆弱性関連情報の届出状況は公開する．

同　2．受付機関基準

(7) 受付機関は，脆弱性に起因する被害の予防に資するため，脆弱性関連情報の届出状況等を公表すること．

問8　ウ

選択肢ア，イ，エは，本問の攻撃の防止とは無関係である．

ア：SOA（Start Of Authority）レコードのシリアル番号の更新は，ゾーンデータが変更されていることを示す．

イ：ホストのIPアドレスの変更を予定している場合は，キャッシュが適切に更新されるように事前にセカンダリDNSサーバがプライマリDNSサーバに問い合わせを行う時間間隔（更新間隔）を短くする．

ウ：正しい．第三者に公開する必要がない情報をゾーン転送してしまわないように，ゾーン転送を許可したDNSサーバを登録する．

エ：DNSラウンドロビンは，一つのドメイン名に複数のIPアドレスを割り当てる負荷分散技術の一つである．トラフィックを複数のIPアドレスのホストに分散させるために用いられる．

問題

問 9

正解 完璧 直前CHECK

ワームの侵入に関する記述のうち，適切なものはどれか．

ア　公開サーバへのワームの侵入は，IDSでは検知できない．
イ　未知のワームの侵入は，パターンマッチング方式で検知できる．
ウ　ワームは，アプリケーションソフトの脆弱性を突いて侵入できる．
エ　ワームは，仮想OS環境内のゲストOSに侵入できない．

問 10

正解 完璧 直前CHECK

ステガノグラフィを説明したものはどれか．

ア　データの複写を不可能にする（コピーできないようにする）技術のことをいう．
イ　データを第三者に盗み見られても解読できないようにするため，決まった規則に従ってデータを変換することをいう．
ウ　文書の正当性を保証するために付けられる暗号化された署名情報のことをいう．
エ　メッセージを画像データや音声データなどに埋め込み，その存在を隠す技術のことをいう．

問 11

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9　ウ

ア：IDS（侵入検知システム）で検知できる．
イ：未知のワームの侵入は，パターンマッチング方式では検知できない．
エ：仮想OS環境内のゲストOSやその上で動作しているアプリケーションに脆弱性があれば侵入できる．

問10　エ

ステガノグラフィ：電子透かしのこと．映像，画像などのデータに見た目ではわからないようにその存在を隠して符号や文字列を埋め込み，専用の閲覧ソフトによって埋め込んだ符号や文字列を確認する．埋め込んだ符号や文字列によりデータが不正にコピーされたものでないかを知ることができる．
ア：コピーガードの説明である．
イ：暗号化の説明である．
ウ：ディジタル署名の説明である．

問11　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．

問題

問 12

正解 完璧 直前CHECK

ダウンローダ型ウイルスがPCに侵入した場合に，インターネット経路でほかのウイルスがダウンロードされることを防ぐ有効な対策はどれか．

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 13

正解 完璧 直前CHECK

ディジタル証明書を使わずに，通信者同士が，通信によって交換する公開鍵を用いて行う暗号化通信において，通信内容を横取りする目的で当事者になりすますものはどれか．

ア　Man-in-the-middle攻撃
イ　war driving
ウ　トロイの木馬
エ　ブルートフォース攻撃

問 14

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与して，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25番への直接の通信を禁止する．

問12　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，この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13　ア

Main-in-the-middle攻撃（中間者攻撃）：暗号通信の間に割り込んで盗聴したり，通信内容に介入する手法．

war driving：セキュリティで保護されていない，あるいは不備のある個人宅や企業内の無線LANのアクセスポイントを求めて，オフィス街などを車で移動するクラッキングの手口．

トロイの木馬：コンピュータの脅威になるソフトウェアのこと．

ブルートフォース攻撃：総当り攻撃のこと．考えられるすべての鍵を試みる方法．

問14　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のこと．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者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照合する．

エ：**OBP25**（Outbound Port 25 Blocking）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ィ対策はどれか.

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SMTP通信を禁止する.

イ　PCからの電子メール送信について，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とは独立したサブミッションポートを使用して，メールサーバ接続時の認証を行う.

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

セキュリティプロトコルSSL/TLSの機能はどれか.

ア　FTPなどの様々なアプリケーションに利用されて，アプリケーション層とトランスポート層（TCP）との間で暗号化する.

イ　MIMEをベースとして，電子署名とメッセージの暗号化によって電子メールのセキュリティを強化する.

ウ　PPTPとL2Fが統合された仕様で，PPPをトンネリングする.

エ　特定のアプリケーションの通信だけではなく，あらゆるIPパケットをIP層で暗号化する.

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電子メール送信を許可する認証方式である．

ア：電子メール広告業者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利用されてきた．

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 ア

SSL/TLSは，クライアントとサーバ間で暗号化するためのプロトコル．WWWやFTPなどのデータを暗号化することができる．**TLS**は公開鍵暗号や秘密鍵暗号，ディジタル証明書，ハッシュ関数などのセキュリティ技術を組み合わせ，データの盗聴や改ざん，なりすましを防ぐことができる．

イ：S/MIMEの説明である．

ウ：L2TPの説明である．

エ：IPsecの説明である．

問題

問 17　正解　完璧　直前CHECK

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　鍵交換プロトコルとして，HMAC-MD5が使用される．

ウ　トンネルモードを使用すると，元のヘッダまで含めて暗号化される．

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17　ウ

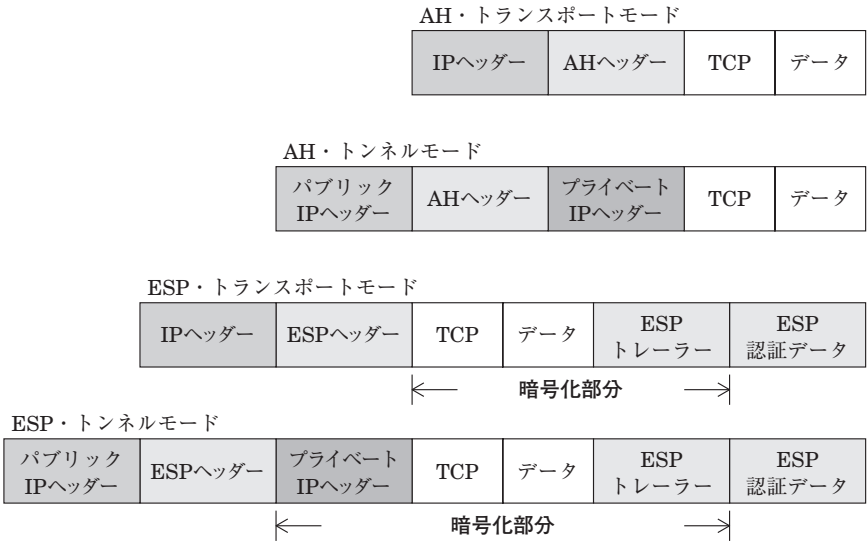
IPsecはインターネットで暗号通信を行うための規格である．IPv6では標準で実装される．

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-MD5は，IPsecのAH（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．

エ：AHでは暗号化はできない．

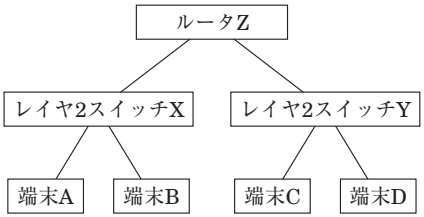


問題

問 18

正解 完璧 直前CHECK

図のような2台のレイヤ2スイッチ，1台のルータ，4台の端末からなるIPネットワークで，端末Aから端末Cに通信を行う際に，送付されるパケットのあて先IPアドレスである端末CのIPアドレスと，端末CのMACアドレスとを対応付けるのはどの機器か．ここで，ルータZにおいてプロキシARPは設定されていないものとする．



ア　端末A　　イ　ルータZ
ウ　レイヤ2スイッチX　　エ　レイヤ2スイッチY

問 19

正解 完璧 直前CHECK

インターネットで電子メールを送信するとき，メッセージの本文の暗号化に共通鍵暗号方式を用い，共通鍵の受渡しには公開鍵暗号方式を用いるものはどれか．

ア　AES　　イ　IPsec　　ウ　MIME　　エ　S/MIME

問18　イ

ルータ：ネットワーク上を流れるデータをほかのネットワークへ中継する機器．OSI参照モデルのネットワーク層（第3層）やトランスポート層（第4層）の一部でプロトコルを解析して転送をする．

プロキシARP：あるホスト宛のARP要求に対して，ルータがそのホストに代わってルータのMACアドレスで応答する方式．サブネットを解釈できないホストが存在するネットワークで利用される．

レイヤ2スイッチ：OSI参照モデルのデータリンク層（第2層）のデータでパケットのあて先を判断して転送するネットワーク中継機器．スイッチングハブと呼ばれ，MACアドレスを見て送り先の端末のみにデータを送信するようにした機器が主流になっている．

端末Aから端末Cへの通信は，端末Aはレイヤ2スイッチXに接続，端末Cはレイヤ2スイッチYに接続されており，端末Aから送出されたパケットの宛て先がスイッチXで配下の端末ではないことから，パケットは上位のルータZへ送信される．ルータZにおいて端末CのMACアドレスとの対応付けが行われ，スイッチYを中継して端末Cへ到達する．

問19　エ

AES：米国で規格化された共通鍵暗号方式．

IPsec：インターネットで暗号通信を行うための規格．

MIME：TCP/IPネットワーク上でやり取りする電子メールで画像，音声，動画を扱うための規格．

S/MIME：RSA公開鍵暗号を用いてメッセージを暗号化して送受信するための電子メール暗号化の標準である．

問題

問 20

正解 □ 完璧 □ 直前CHECK □

192.168.1.0/24のネットワークアドレスを，16個のサブネットに分割したときのサブネットマスクはどれか．

ア　255.255.255.192　　イ　255.255.255.224
ウ　255.255.255.240　　エ　255.255.255.248

問 21

正解 □ 完璧 □ 直前CHECK □

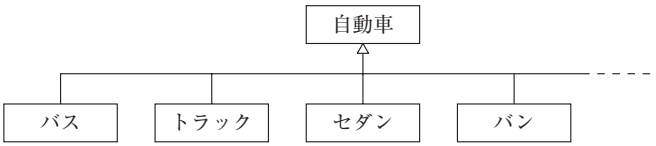
データマイニングツールに関する記述として，最も適切なものはどれか．

ア　企業内で発生する情報を主題ごとに時系列で蓄積することによって，既存の情報システムだけでは得られない情報を提供する．
イ　集計データを迅速かつ容易に表示するなど，利用者に対して様々な情報分析機能を提供する．
ウ　大量に蓄積されたデータに対して統計処理などを行い，法則性の発見を支援する．
エ　利用者が情報を利用するための目的別データベースであり，あらかじめ集計処理などを施しておくことによって検索時間を短縮する．

問 22

正解 □ 完璧 □ 直前CHECK □

次のクラス図におけるクラス間の関係の説明のうち，適切なものはどれか．



ア　“バス”，“トラック”などのクラスが“自動車”クラスの定義を引き継ぐことを，インスタンスという．
イ　“バス”，“トラック”などのクラスの共通部分を抽出し“自動車”クラスとして定義することを，汎化という．
ウ　“バス”，“トラック”などのクラスは，“自動車”クラスに対するオブジェクトという．
エ　“バス”，“トラック”などのそれぞれのクラスの違いを“自動車”クラスとして定義することを，特化という．

問20　ウ

サブネットマスク：ネットワークの識別に利用されるネットワークアドレス部を定義する32ビットの数値．サブネットマスク値とIPアドレスのビットの論理積を計算することによりIPアドレスのネットワークアドレス部を取得できる．

192.168.1.0/24のアドレスで，サブネットマスクが255.255.255.0であるから，左から24ビットがネットワーク部，残り8ビットがホスト部である．ネットワーク自体やブロードキャストアドレスを含めて28＝256台のホストの割当てができる．選択肢のサブネットマスクのホスト数から，分割するサブネット数は下記になる．

選択肢	サブネットマスク	第4オクテットの計算	ホスト数	サブネット数
ア	255.255.255.192	256－192＝64	64個	256／64＝4
イ	255.255.255.224	256－224＝64	32個	256／32＝8
ウ	255.255.255.240	256－240＝64	16個	256／16＝16
エ	255.255.255.248	256－248＝8	8個	256／8＝24

問21　ウ

データマイニング：大量に蓄積されるデータを解析し，その中に潜む項目間の相関関係やパターンなど法則性を探し出す技術．

ア：**データウェアハウス**に関する記述である．

イ：**OLAP**（OnLine Analytical Processing）

エ：**データマート**に関する記述である．

問22　イ

ア：**継承**（インヘリタンス）である．**インスタンス**はデータの値そのもののことを示す．

イ：複数のオブジェクトから共通している概念を抽出し，より抽象的なオブジェクトを導出することを**汎化**という．

ウ：“バス”，“トラック”などのクラスは**サブクラス**である．

エ：**特化**は汎化の対になる言葉であり，具象化することを意味する．“自動車”クラスに対して個々のオブジェクトの違いにより“バス”，“トラック”などそれぞれのクラスとして定義することを特化という．

問 23

正解 □ 完璧 □ 直前CHECK □

SOA（Service Oriented Architecture）の説明はどれか．

ア　Webサービスを利用するためのインタフェースやプロトコルを規定したものである．
イ　XMLを利用して，インターネット上に存在するWebサービスを検索できる仕組みである．
ウ　業務機能を提供するサービスを組み合わせることによって，システムを構築する考え方である．
エ　サービス提供者と委託者との間でサービスの内容，範囲及び品質に対する要求水準を明確にして，あらかじめ合意を得ておくことである．

問 24

正解 □ 完璧 □ 直前CHECK □

情報システムの設計において，フェールソフトが講じられているのはどれか．

ア　UPS装置を設置することで，停電時に手順どおりにシステムを停止できるようし，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で，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 □

“情報セキュリティ監査基準”の位置付けはどれか．

ア　監査人が情報資産の監査を行う際に判断の尺度として用いるべき基準であり，監査人の規範である．
イ　情報資産を保護するためのベストプラクティスをまとめたものであり，監査マニュアル作成の手引書である．
ウ　情報セキュリティ監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的とした監査人の行為規範である．
エ　組織体が効果的な情報セキュリティマネジメント体制を構築し，適切なコントロールを整備，運用するための実践規範である．

問23　ウ

SOA：サービス指向アーキテクチャは，サービスの集まりとしてシステムを構築する手法である．ここで，サービスとは外部から標準化された手順で呼び出すことができる一まとまりのソフトウェアの集合であり，各サービスがXMLで記述されたメッセージをSOAPでやり取りし，連携して動作する．

ア：**SOAP**（Simple Object Access Protocol）の説明である．

イ：**UDDI**（Universal Description, Discovery, and Integration）の説明である．

エ：**SLA**（Service Level Agreement）の説明である．

問24　ウ

フェールソフト：情報システムの一部に障害が発生した際に，故障した個所を破棄あるいは切り離すなどして障害の影響を防ぎ，最低限のシステムの稼動を続けるための技術．

フォールトトレランス：システムに障害が発生したときに，正常な動作を保ち続ける能力を持たせる設計．

フェールセーフ：故障や操作ミス，設計上の不具合などの障害が発生することを想定しておき，被害を最小限にとどめる設計．

ア：フォールトトレランスに関する記述である．

イ，エ：フェールセーフに関する記述である．

問25　ウ

情報セキュリティ監査基準の前文に，『情報セキュリティ監査基準とは，情報セキュリティ監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的とした監査人の行為規範である．本監査基準は，監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」，監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」，監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」からなっている．』とある．

ア，イ，エ：情報セキュリティ管理基準の説明である．