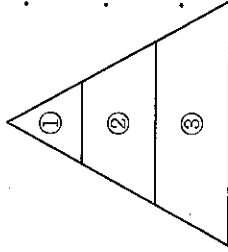


2.3 情報セキュリティ(3)

問 1 【解答ア】

情報セキュリティの文書を詳細化の順に上から並べると、次のようになる。



…情報セキュリティ「基本方針」

：組織としての統一かつ基本的な考え方や理念を表したもの

…情報セキュリティ「対策基準」

：基本方針を実践するための遵守事項や基準を記述したもの

…情報セキュリティ「対策実施手順」

：情報セキュリティ対策の具体的な実施手順を記述したもの

なお、基本方針と対策基準をまとめて「情報セキュリティポリシー」という場合もある。

問 2 【解答ウ】

情報セキュリティマネジメントシステムにおいては、情報セキュリティマネジメントの三大要素（機密性、完全性、可用性）を維持することが求められる。このうち、「可用性」は、必要などきに、必要な資産（データ）に確実にアクセスできる特性である。したがって、「認可された利用者が、必要などきに情報にアクセスできること」が該当する。

ア：ソフトウェア製品の品質特性の一つである“機能性”の説明である。

イ：“完全性”（資産（データ）の正確さ・完全さを保護する特性）の説明である。

エ：“機密性”（認可されていない相手には、情報を非公開とする特性）の説明である。

問 3 【解答エ】

情報セキュリティマネジメントシステム（ISMS：Information Security Management System）は、“計画（Plan）”、“実行（Do）”、“点検（Check）”、“処置（Act）”のPDCAサイクルで進められる。

・ P（計画 [Plan]）

：情報セキュリティ基本方針などを策定する。

・ D（実行 [Do]）

：情報セキュリティ対策基準や情報セキュリティ対策実施手順を決めて運用する。

・ C（点検 [Check]）

：ISMSを監視／評価する。

・ A（処置 [Act]）

：導入したISMSを見直して改善する。（正解）

問 4 【解答イ】

・ リスク対策

：リスクが発生したときの対応について優先順位を決め、損失と対策費用の関係（コストパフォーマンス）などから、リスクへの対応策を決定する。

・ リスク特定

：資産を調査して、発生する可能性のあるリスクを資産ごとに洗い出す。（正解）

・ リスク評価

：リスクが発生した場合の損失などによる、経営上の影響範囲などを評価する。

・ リスク分析

：リスクの種類や発生頻度、強度（リスクに対する強さ）などを分析する。

問3 【解答エ】

・キーロガー

：キーボード入力を記録する仕組み（ソフトウェア）を利用して，他人が入力した情報（パスワードなど）を不正に入手する攻撃である。

・ゼロデイ攻撃

：ベンダ企業がソフトウェアの脆弱性（セキュリティホール）を公表した場合に，その修正プログラムが提供される前に脆弱性を悪用して行われる攻撃である。

・パッパアオーパーパフロア攻撃

：長い文字列などを送り続け，プログラムが確保したメモリ領域（バッファ）をあふれさせることにより，プログラムのアクセス権を支配し，誤作動を起こさせる攻撃である。

・フィッシング

：実在する会社を装って偽電子メールを送ったり，DNSキャッシュポイズニング（DNSサーバのキャッシュ情報を改ざんする攻撃）を用いたりして，利用者を偽のWebページに誘導し，情報（パスワードなど）を入力させて不正に入手する攻撃である。（正解）

問4 【解答イ】

スパムメールとは，受信者の承諾なしに不特定多数に一方的に送りつけられる広告メールのことである。迷惑メールの一種で，広告や勧誘などを目的としたダイレクトメールなどが該当する。

ア：同報メールやメールマガジンに関する説明である。

ウ：オプトインメールに関する説明である。

エ：チェーンメールに関する説明である。チェーンメールも迷惑メールに分類される。

問5 【解答イ】

ランサムウェアとは，「感染すると勝手にファイルやデータの暗号化などを行って，正常にデータにアクセスできないようにし，元に戻すための代金を利用者に要求するソフトウェア」である。ランサムとは“身代金”を意味する言葉である。

ア：ウイルス対策ソフトに関する説明である。

ウ：OS（オペレーティングシステム）に関する説明である。

エ：日本語IME（Input Method Editor）に関する説明である。

問6 【解答エ】

DoS（Denial of Service）攻撃は，標的のサーバに大量のデータを送信し続け，サーバのCPU，メモリなどに過剰な負荷をかける攻撃である。その結果として，「サービスの提供が阻害される」という被害が生じることになる。

問7 【解答ア】

クロスサイトスクリプティング（XSS：Cross Site Scripting）は，悪意をもったスクリプトを，脆弱性のある標的サイト経由で利用者に送り，その標的サイトにアクセスした利用者にスクリプトを実行させて，情報を盗み出す攻撃である。Webサイトの運営者が意図しないスクリプトを含むデータであっても，利用者のブラウザに送ってしまう脆弱性を利用している。

イ：OSコマンドインジェクション攻撃に関する記述である。

ウ：パスワードドリフト攻撃に関する記述である。

エ：IPスプーフィングに関する記述である。

問6 【解答ア】

ソーシャルエンジニアリングは、代表的な人的脅威の一つであり、日常的、一般的な手段で情報を盗み取る行為である。ごみ箱に捨てられているメモから重要な情報を盗む“トラッキング”や、第三者が、あたかも本人であるかのように装って、暗証番号やパスワードを聞き出す“なりすまし”などがある。したがって、「運用担当者のセキュリティ意識が低い」と、ソーシャルエンジニアリングによる被害に結びつきやすい状況であるといえる。

イ：物理的脅威による被害に結びつきやすい状況である。

ウ：クラッキングによる被害に結びつきやすい状況である。

エ：盗聴による被害に結びつきやすい状況である。

問7 【解答ア】

ア：ハードディスク全体を16進数の00やFF、または乱数で複数回上書きしておく、データを物理的に削除したことになるので、情報漏えいを防ぐ方法として最も確実な方法である。(正解)

イ：ハードディスクを論理フォーマットしてもデータを物理的に削除したことにはならないので、ハードディスクに記録された情報を読み取られる危険性がある。

ウ：ファイルやフォルダをゴミ箱に捨ててから空にしてもデータを物理的に削除したことにはならないので、ハードディスクに記録された情報を読み取られる危険性がある。

エ：ハードディスクにパスワードロック（一般にATAパスワードと呼ばれる）をかけることで、情報漏えいを防ぐ効果が期待できる。しかし、このようなロックを解除するツールやスキルも存在しているため、情報漏えいを防ぐ最も確実な方法とはいえない。（正解）

2.3 情報セキュリティ(2)

情報セキュリティの脅威(2)

問1 【解答ウ】

- ・アドウェア
： 広告を目的として配布される、一般的には無償のソフトウェアである。
- ・シェアウェア
： 一定の試用期間後に、利用を続ける場合に料金を支払う必要のあるソフトウェアである。
- ・マルウェア
： 悪意をもって作成されたソフトウェア（プログラム）の総称である。コンピュータウイルスや、ワーム、ボット、スパイウェアなどがある。(正解)
- ・ミドルウェア
： OSと応用ソフトウェア（アプリケーションソフトウェア）の中間に位置付けられる、複数の応用ソフトウェアが共通して利用するOSの基本機能を提供するソフトウェアである。

問2 【解答エ】

マクロとは、処理手順をあらかじめ登録（定義）しておき、必要ときに呼び出して実行させる、ワープロソフトや表計算ソフトの機能である。マクロウイルスは、このマクロ機能を利用したウイルスであり、「ワープロソフトや表計算ソフトのデータファイルに感染する。」

ア：ボットに関する説明である。

イ：スパイウェアに関する説明である。

ウ：トロイの木馬に関する説明である。

問2 【解答ア】

・誤操作

：操作を間違えて、データを消去したりしてしまうことである。処理（操作）をうっかり間違えた結果として発生した現象なので、この脅威に該当する。（正解）

・破壊

：悪意のある第三者による妨害行為、破壊行為などによって、機器が壊れて使えなくなることである。

・破損

：情報が保存されているPCやUSBメモリなどを、使用中に壊してしまうことである。

・紛失

：情報が保存されているPCやUSBメモリなどを、置き忘れたり、盗まれたりしてなくなってしまうことである。

問3 【解答ア】

・クラッキング

：悪意をもって他人のPCに侵入し、データを盗み見たり、破壊したりする行為である。クラッキングを行う人をクラッカーという。（正解）

・ショルダハッキング

：パスワードを入力している人のキーボードの操作や画面に表示された情報を、肩越しからのぞいて盗み見る行為である。

・トラッキング（スキベンジング）

：ごみ箱に捨てられたメモから、重要な情報を盗んだりする行為である。

・標的型攻撃

：ある特定の組織や人間をターゲット（標的）として攻撃する行為である。

問4 【解答ア】

ア：大雨という自然災害が原因なので、物理的脅威に分類される。（正解）

イ：大量のデータを送りつけるというコンピュータ技術を利用した攻撃（脅威）なので、技術的脅威に分類される。

ウ：ネットワークを介して社内サーバに侵入するというコンピュータ技術を利用した攻撃（脅威）なので、技術的脅威に分類される。

エ：社員が電子メールの宛先を間違えるという誤操作が原因なので、人的脅威に分類される。

問5 【解答エ】

ア：内部からの不正アクセス（アクセス権をもっていない第三者が、ネットワークに侵入すること）もあるので、外部からの侵入を阻止するだけでは事前対策として不十分である。

イ：発生する自然災害（地震、洪水など）を想定して、バックアップサイトの準備や定期的なバックアップ計画の立案など、適切な事前対策を講じるべきである。

ウ：情報の漏えいや機器の紛失などの脅威もあるので、データのバックアップだけでは事前対策として不十分である。

エ：脅威の種類を理解し、それぞれの資産への影響（予想損失額など）を考慮して、事前に対策を講じておくことが大切である。予想損失額よりも対策コストのほうが高いような場合、あえて事前対策を講じないということもある。（正解）

問7 【解答イ】

VoIP (Voice over Internet Protocol) は、音声信号 (アナログ信号) をデジタル信号に変換して、パケット単位に分割して伝送する技術である。VoIPを利用しているIP電話では、インターネットによるリアルタイム通話を実現している。

ア : SaaS (Software as a Service) などに関する説明である。

ウ : VPN (Virtual Private Network) に関する説明である。

エ : DNS (Domain Name System) に関する説明である。

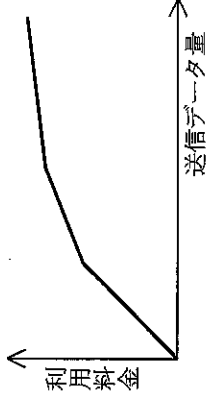
問8 【解答ア】

従量制は、送信データ量 (パケット数) によって利用料金が決まる課金方式である。送信データ量が多くなるほど、利用料金も比例して高くなるので「a」のような右上がりの直線になる。

b : 携帯電話の契約などで用いられる段階的定額制を表している。

c : 定額制の課金方式を表している。

d : 送信データ量が増えるほど、利用料金が少なくなるということはない。なお、コンピュータシステムの課金などでは、使用量が多くなるにつれて利用金額 (単価) が安くなる通減課金方式というものもある。通減課金方式のグラフは、次のようになる。



2.3 情報セキュリティ(1)

情報セキュリティの脅威(1)

問1 【解答ウ】

脅威とは、システムまたは組織、人間に損害を与える可能性があるもの (原因) である。脅威は、人的脅威、物理的脅威、技術的脅威に分類される。

・人的脅威 : 人間の行為 (悪意の有無は問わない) が原因となる脅威である。

・物理的脅威 : 機器自体や機器が設置された建物などに対する脅威である。

・技術的脅威 : 悪意のある第三者が、コンピュータ技術を利用して攻撃してくる脅威である。なお、脅威が与える損害には組織に対する経済的な損失も含まれるので、あえて情報セキュリティの脅威に「経済的脅威」という分類はない (ある意味で、すべての脅威が経済的脅威である)。

問3 【解答イ】

- ・ADSL (Asymmetric Digital Subscriber Line)
：アナログ電話回線を利用した，上りと下りの通信速度が異なる回線サービスである。
- ・FTTH (Fiber To The Home)
：高速大容量の光ファイバケーブルを利用した回線サービスである。伝送速度は10M～100Mビット/秒と非常に高速である。(正解)
- ・HDSL (High-bit-rate Digital Subscriber Line)
：アナログ電話回線を利用した，上り・下りの通信速度が同じ回線サービスである。
- ・ISDN (Integrated Service Digital Network)
：音声通信，データ通信など複数の通信サービスを統合したデジタル交換網である。

問4 【解答ウ】

- ・anonymous FTP
：ユーザIDに“anonymous (匿名)”と入力すると，誰でも利用できるFTPサービスである。
- ・PIAFS (PHS Internet Access Forum Standard)
：PHSを使った通信プロトコルである。
- ・デザリング
：携帯電話回線に接続された携帯情報端末（タブレット端末やスマートフォン，携帯電話など）を利用して，ノート型PCなどをインターネットに接続する方法である。(正解)
- ・ルーティング
：ルータなどで利用される経路選択のことである。

問5 【解答イ】

- ・IP電話
：インターネットを利用した音声通信サービスである。
- ・VPNサービス
：インターネットなどで利用されている公衆回線を，専用線のように使用できる仮想私設通信網 (VPN: Virtual Private Network) を提供するサービスである。(正解)
- ・Webサービス
：個人や企業がインターネットのWebサーバに登録した情報を，誰でもPCにダウンロードしてWebブラウザによって見ることができサービスである。
- ・モバイル通信
：携帯電話やノート型PCを利用した移動体通信サービスである。

問6 【解答エ】

- ア：ADSL (Asymmetric Digital Subscriber Line) 回線では，すべてアナログ回線（メタル）を使用する。
- イ：ADSL回線では，モデムから収容局までの距離が長くなるほど通信速度が低下する。
- ウ：アナログ電話とPCは別の周波数帯域を使用しているのので，アナログ電話とPCを同時に利用しても単独利用より通信速度が低下することはない。
- エ：ADSL回線は，アナログ回線（メタル）を利用した，上りと下りの伝送速度が異なる回線サービスである。伝送速度は，上り（アップロード時）が512k～5Mビット/秒程度，下り（ダウンロード時）が1.5～50Mビット/秒程度であり，ダウンロード時のほうが速い。(正解)

問5 【解答ウ】

電子メールの宛先入力欄には、Toの他にCc (Carbon copy) やBcc (Blind carbon copy) がある。Cc及びBccは、宛先(To)に送信する電子メールと同じ内容の電子メールを複写して送信するための、メールアドレスの指定である。Ccに指定したメールアドレスは、受信した全ての電子メールに表示されるが、「Bccに指定した宛先のメールアドレスは、他の宛先には通知されない。」

問6 【解答ア】

フィードとは、Webサイトの更新情報やページの概要などをまとめたRSSやAtomフォーマットのデータのことである。Webページにおいてフィードアイコンが表示されている場合、そのWebサイトの更新情報や概要などをまとめたフィードを提供していると説明している。

問7 【解答エ】

cookie (クッキー) は、Webサーバにアクセスしてきたブラウザに、Webサーバからの情報 (ユーザー情報、最終セッション確立日/時間など) を一時的に保存する仕組みである。Webサーバが、これらの情報から利用者を識別することで、「利用者が過去にアクセスしたWebサイトに再度アクセスしたときに、その利用者に合わせた設定でWebページが表示される。」ただし、これらの情報には個人情報が含まれることがあるので、不特定多数が利用するPCなどでは、cookieを消去して情報が盗まれないようにする必要がある。

ア：メールアドレスの利便性である。

イ：リスティング広告 (検索エンジン連動型広告) の利便性である。

ウ：トラッキング機能の利便性である。

2.2 ネットワーク(6)

通信サービス

問1 【解答ア】

- ・ISP (Internet Service Provider ; インターネット接続サービス事業者)
 - ：インターネットへの接続サービスを提供する回線事業者である。(正解)
- ・NIC (Network Information Center)
 - ：IPアドレスが世界中で重複しないように管理している団体である。
- ・SI (System Integrator ; システムインテグレータ)
 - ：情報システムの企画・構築・運用などの業務を一括して請け負うシステムインテグレーション (SI : System Integration) を行う事業者である。
- ・W3C (World Wide Web Consortium)
 - ：WWW (World Wide Web) で使用される、さまざまな技術標準を定める組織である。

問2 【解答エ】

- ア：一般的な課金方式としては、送信したパケット数によって決まる従量制が使われる。ただし、携帯電話などのモバイル通信では、料金プランを定額としている場合もある。
- イ：パケット単位に伝送するため、送信順序と受信順序が異なる場合がある。ただし、パケットごとに番号が割り振られているので、受信側で正しい順序に並べ替えることができる。
- ウ：データの送信では、パケット単位に伝送経路を決定する。
- エ：パケット通信は、伝送するデータを一定の長さに分割したパケットという単位で送信する回線サービスである。(正解)

2.2 ネットワーク(5)

インターネットのサービス

問1 【解答エ】

- ・オプトインメール
: 広告受信許諾 (オプトイン) 者を対象に送信される電子メールである。
- ・オンラインストレージ
: インターネットを利用した, ファイル保管場所の貸出サービスである。
- ・フィード
: RSS (RDF Site Summary) 形式で作成された更新情報である。
- ・メールボックス
: メールサーバにある個人専用の電子メール保管場所である。利用者は, メールボックスに届いた電子メールをPCで受信し, 好きなときに読むことができる。(正解)

問2 【解答ウ】

メールングリストとは, あらかじめ作成してあるメールアドレスのリストである。同じ内容の電子メールを送れる「同報メールを送信する相手だけのメールアドレスを登録してある。」

- ア: ホワイトリストに関する説明である。
- イ: ブラックリストに関する説明である。
- エ: メールソフトのアドレス帳に関する説明である。

問3 【解答ア】

ア: CGI (Common Gateway Interface) は, Webサーバなどで, Webページから入力されたデータの処理プログラムを起動する仕組みである。(正解)

イ: RSSリーダーは, ページの見出しや要約, 更新時刻などのメタデータを構造化して記述する, RSS形式で作成された更新情報 (フィード) を収集するソフトウェアである。

ウ: クローラは, インターネット上の情報を収集してデータベース化する処理を行うプログラムである。この記述は, アプリケーションサーバに関するものである。

エ: サーチエンジンとは, Webサービスの一つである, 情報を検索するサイト (検索サイト) で処理を行うプログラムである。

問4 【解答ウ】

- ・DHCP (Dynamic Host Configuration Protocol) サーバ
: ネットワークに接続された機器の起動時または送信要求時に, IPアドレスを動的に割り当てるサーバである。
- ・DNS (Domain Name System) サーバ
: URLやメールアドレスをIPアドレスに変換するサービスを提供するサーバである。
- ・FTP (File Transfer Protocol) サーバ
: ファイルをダウンロードしたり, アップロードしたりするために, ファイル転送サービスで用いられるサーバである。(正解)
- ・PROXYサーバ
: LAN内のPCに代わって, 外部ネットワークにアクセスするサーバである。

問3 【解答イ】

ア：IPv6の考え方（ネットワークアドレスやサブネットマスクなど）は、ほとんどIPv4と同じなので、IPv4と共存する仕組みやプロトコルが提案されている。

イ：IPv6 (Internet Protocol version 6) は、IPv4のビット数 (32ビット) を拡張したインターネットプロトコルである。「IPアドレスのビット数がIPv4の4倍 (128ビット) ある」ので、16ビットずつコロン (:) で区切って、それぞれを16進数で表記する。(正解)

ウ：IPv6では、パケットの暗号化や認証を行うセキュリティプロトコルであるIPsec (Security Architecture for Internet Protocol) を標準仕様としている。

エ：IPv6のIPアドレスは、128ビットのIPアドレス (0と1の組合せ) を16ビットずつコロン (:) で区切って、それぞれを16進数 (数値) で表記する。

問4 【解答エ】

URL (Uniform Resource Locator) は、インターネット上の「Webページの場所を示すための表記法 (アドレス) である。」URLは、アクセスするためのプロトコル、ホスト名 (機器の名称)、ドメイン名 (組織やネットワークの名称) で構成される (ホスト名を含めて、ドメイン名という場合もある)。

ア：HTTP (Hypertext Transfer Protocol) に関する説明である。

イ：RSS (RDF Site Summary) で記述されたメタセージに関する説明である。

ウ：HTML (Hypertext Markup Language) に関する説明である。

問5 【解答イ】

NAT (Network Address Translation) の機能は、プライベートIPアドレスとグローバルIPアドレスを1対1で変換することである。

ア、イ：グローバルIPアドレスとドメイン名 (URL) 又はメールアドレスの相互変換を行うのは、DNS (Domain Name System) の機能である。

ウ：プライベートIPアドレスとMACアドレスの相互変換を行うのは、ARP (Address Resolution Protocol) やRARP (Reverse Address Resolution Protocol) の機能である。

問6 【解答エ】

DNS (Domain Name System) サーバは、URL (Uniform Resource Locator) やメールアドレスをIPアドレスに変換するサーバである。URLはホスト名やドメイン名等で構成されているため、DNSサーバの機能は「問合せのあったホスト名のIPアドレスを回答する」ことになる。

ア：ルータの機能に関する記述である。

イ：プロキシサーバの機能に関する記述である。

ウ：ARP (Address Resolution Protocol) の機能に関する記述である。

問7 【解答エ】

「ネットワーク設定情報」の最後に“PCは、DHCPサーバを使用すること”とある。DHCP (Dynamic Host Configuration Protocol) サーバは、ネットワークに接続された機器の起動時または送信要求時に、IPアドレスを動的に割り当てるサーバである。したがって、PCにIPアドレスを個別に設定するのではなく、DHCPサーバから「IPアドレスを自動的に取得する設定にする。」

ア：IPアドレスとして、ネットワークアドレス (192.168.1.0) と同じものは設定できない。

イ：IPアドレスとして、デフォルトゲートウェイ (192.168.1.1) と同じものは設定できない。

ウ：IPアドレスは、DHCPサーバを使用して自動的に取得して設定するので、独自に設定することはない。

問5 【解答イ】

HTTPS (HyperText Transfer Protocol over SSL/TLS) は、Webサーバに登録されているホームページなどのコンテンツを、ブラウザで閲覧するために使用されるプロトコルであるHTTPに、盗聴などを防ぐセキュリティ機能を追加したプロトコルである。HTTPSを用いてブラウザとWebサーバ間で通信を行うとき、通信内容が暗号化されるのは「ブラウザとWebサーバ間」である。

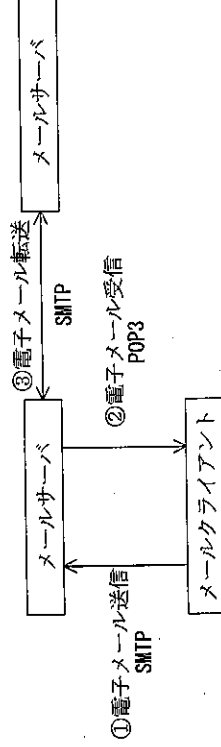
問6 【解答ウ】

・SMTP (Simple Mail Transfer Protocol)

：PCからメールサーバへの電子メールの送信 ① や、メールサーバ間での電子メールの転送 ③ に使用されるプロトコルである。

・POP3 (Post Office Protocol version 3)

：PCが、メールサーバから電子メールを受信 ② するプロトコルである。
したがって、図の電子メール送受信で利用されるプロトコルの組合せは、次のようになる。



2.2 ネットワーク(4)

インターネットの仕組み

問1 【解答エ】

IPアドレスは、「ネットワークに接続された機器 (PCやサーバなど) を特定するためのアドレス (値) である。」現在の標準的なインターネットプロトコルであるIPv4では、32ビットのIPアドレスを8ビットずつに区切って、四つの10進数で「204. 51. 85. 170」のように表現する。

ア：ポート番号に関する説明である。

イ：メールアドレスに関する説明である。

ウ：MACアドレスに関する説明である。

問2 【解答エ】

サブネットマスクは、ネットワークアドレス (サブネットアドレス) を取り出すために、取り出したい部分を'1'にしたビット列である。

したがって、IPアドレスの上位20ビットをサブネットアドレスとする場合のサブネットマスクは、次のように上位20ビットを'1'にしたビット列となる。

上位20ビットを'1'にしたビット列：	11111111	11111111	11110000	00000000
	↓	↓	↓	↓
サブネットマスク：	「255.	255.	240.	0」

2.2 ネットワーク(3)

問 1 【解答エ】

- ・FTP (File Transfer Protocol)

：インターネットのサーバからファイルをダウンロードしたり、インターネットのサーバにファイルをアップロードしたりする、ファイル転送用のプロトコルである。

- ・HTTP (HyperText Transfer Protocol)

：Webサーバに登録されているホームページなどのコンテンツ (HTML文書) を、Webブラウザで閲覧するために使用されるプロトコルである。

- ・SMTP (Simple Mail Transfer Protocol)

：PCからメールサーバへの電子メールの送信や、メールサーバ間での電子メールの転送に使用されるプロトコルである。

- ・TCP/IP (Transmission Control Protocol/Internet Protocol)

：インターネットを中心に利用されている、デファクトスタンダード (業界標準) の通信プロトコル体系である。TCP/IPは、AP層 (アプリケーション層)、TCP層、IP層、NI層 (ネットワークインタンフウェア層) の4階層に分類 (体系化) されている。(正解)

問 2 【解答ア】

MIME (Multipurpose Internet Mail Extensions) は、電子メールのメッセージヘッダを拡張して、テキストデータのほかに、画像、音声、動画などのデータも送信できるようにしたプロトコルである。利用例としては、「画像ファイルを電子メールに添付して送信する」などが該当する。

イ：IMAP (Internet Message Access Protocol) の利用例である。

ウ：NTP (Network Time Protocol) の利用例である。

エ：FTP (File Transfer Protocol) の利用例である。

問 3 【解答エ】

- ・FTPS (FTP over SSL/TLS)

：FTPに、セキュリティ機能を追加したプロトコルである。

- ・HTTPS (HTTP over SSL/TLS)

：HTTPに、盗聴などを防ぐセキュリティ機能を追加したプロトコルである。

- ・S/MIME (Secure MIME)

：MIMEに、暗号化などのセキュリティ機能を追加したプロトコルである。

- ・SSL (Security Sockets Layer)

：データの暗号化機能や、電子証明書などを使用した利用者 (またはWebサーバ) 認証機能を備えたセキュリティプロトコルである。Webサーバが送信した電子証明書などを利用して、クライアントPC側でWebサーバを認証するために用いられる。(正解)

問 4 【解答イ】

ポート番号は、コンピュータが「通信相手のアプリケーションソフトウェア (プログラム)」を識別したり、サービスを提供するプログラムを識別したりするための番号である。

ア：LANカードは、MACアドレスによって識別される。

ウ：通信相手のコンピュータは、IPアドレスによって識別される。

エ：アクセスポイントは、ESSID (Extend Service Set Identifier) などによって識別される。

問5 【解答イ】

“10BASE5”は、伝送速度が10Mビット/秒のLANである。ただし、伝送速度はあくまでも標準速度であり、実際には通信回線の伝送効率を考慮して、実効伝送速度を求める必要がある。

$$\text{実効伝送速度} = \text{伝送速度} \times \text{伝送効率}$$

$$= 10\text{Mビット/秒} \times 0.9$$

$$= 9\text{Mビット/秒}$$

したがって、1秒間に実際に伝送できるのは「9」Mビットである。

問6 【解答エ】

ア：スイッチは、論理的に一つのLANとして扱われるので、異なるネットワーク（インターネットなどの外部ネットワーク）と接続することはできない。

イ：スイッチは、論理的に一つのLANとして扱われるので、同報通信の場合は、すべての端末にパケットが送信される。

ウ：スイッチは、論理的に一つのLAN（同じネットワーク）として扱われる。

エ：スイッチは、MACアドレスによるフィルタリング機能（ストアアンドフォワード）をもった接続装置であるので、中継する必要のないデータを識別して通過を制限できる。（正解）

問7 【解答ウ】

プロキシサーバは、LAN内のPCに代わって、外部ネットワークにアクセスするサーバである。プロキシサーバが「内部ネットワークから外部ネットワークへのアクセスを代行することで、外部ネットワークからはこのサーバしか見えないようにする」ことによって、内部ネットワークに対する直接的な攻撃を防ぐことができる。

ア：DHCP (Dynamic Host Configuration Protocol) サーバを導入する目的である。

イ：DNS (Domain Name System) サーバを導入する目的である。

エ：SSL (Secure Sockets Layer) などのセキュリティブロトコルを導入する目的である。

問8 【解答エ】

伝送速度と伝送効率から求めた実効伝送速度を用いて、データ転送時間を求める。このとき、単位の変換（MとG、ビットとバイト）があることに注意する。

手順1 伝送速度と伝送効率から実効伝送速度を求める。

$$\text{実効伝送速度} = 100\text{Mビット/秒} \times 0.8$$

$$= 80\text{Mビット/秒}$$

手順2 転送するデータ量をビットで求める。

$$\text{転送するデータ量} = 10\text{Gバイト} \times 8\text{ビット/バイト}$$

$$= 80\text{Gビット}$$

手順3 ファイルを転送するために必要な時間（データ転送時間）を求める。

$$\text{データ転送時間} = \text{転送するデータ量} \div \text{実効伝送速度}$$

$$= 80\text{Gビット} \div 80\text{Mビット/秒}$$

$$= 80 \times 10^9 \text{ビット} \div (80 \times 10^6 \text{ビット/秒})$$

$$= 1 \times 10^3 \text{秒}$$

$$= \text{「1,000」秒}$$