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ィ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。
・テザリング
　：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るサービスである。
・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7　【解答イ】

VoIP（Voice over Internet Protocol）は，音声信号（アナログ信号）をディ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。

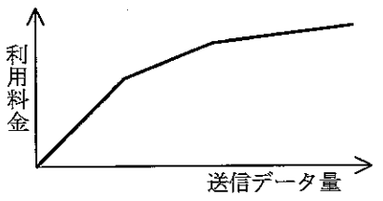
問8　【解答ア】

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）が安くなる逓減課金方式というものもある。逓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し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。
・トラッシング（スキャベンジング）
　：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“トラッシング”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と，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くなっている。

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，必要な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。
・バッファオーバフロー攻撃
　：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】

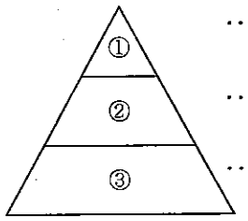
クロスサイトスクリプティング（XSS：Cross Site Scripting）は，悪意をもったスクリプトを，脆弱性のある標的サイト経由で利用者に送り，その標的サイトにアクセスした利用者にスクリプトを実行させて，情報を盗み出す攻撃である。Webサイトの運営者が意図しないスクリプトを含むデータであっても，利用者のブラウザに送ってしまう脆弱性を利用している。

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：パスワードリス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。

2．3　情報セキュリティ(3)　　情報セキュリティ管理

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」
　　：組織としての統一的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”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，必要なときに，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，必要なと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５　【解答エ】

情報セキュリティポリシは，情報セキュリティに対する組織としての考え方を明文化したものである。「組織内の複数の部門で異なる情報セキュリティ対策を実施する場合でも，情報セキュリティ基本方針は組織全体で統一させるべきである。」

ア：情報セキュリティに関する規則や手順は，情報システムや管理部門ごとに策定する。

イ：情報セキュリティに関する規則や手順を社外に公開する必要はない。

ウ：情報セキュリティ基本方針も組織の状況や業務内容に合わせるべきであり，業界標準の雛形をそのまま採用する必要はない。

問６　【解答イ】

ISMS（Information Security Management System）は，企業や組織が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）を確保・維持するために，情報セキュリティポリシに基づいてセキュリティレベルの設定やリスクアセスメントなどを継続して行い，情報資産を正しく，安全に運用するための枠組みである。

a：“計画（Plan）”，“実行（Do）”，“点検（Check）”，“処置（Act）”のPDCAサイクルで進め，改善と活動を継続する。（正しい）

b：組織の経営層が情報セキュリティポリシを策定し，その基本方針に基づいて具体的な実施手順などを策定するトップダウンの活動である。

c：導入及び活動は経営層を頂点とし，組織的に取り組むべきである。（正しい）

d：改善と活動を継続し，終了することはない。

したがって，ISMSの特徴として適切なのは「a，c」である。

問７　【解答エ】

リスク回避は，リスクを避けるために，リスクの発生源となるものの使用を中止するか，代替する対応方法である。したがって，「リスクの大きいサービスから撤退した」ことが，該当する。

ア：リスク予防（リスク低減）に該当する事例である。

イ：リスク移転に該当する事例である。

ウ：リスク受容に該当する事例である。

2.3　情報セキュリティ(4)　　情報セキュリティ対策

問１　【解答エ】

社内の情報セキュリティ教育は，情報セキュリティポリシを遵守させるために社員を教育することで，情報セキュリティに関する個人の意識を高めることを目的としている。教育の「内容は，社員の担当業務，役割及び責任に応じて変更する」ことが重要である。

ア：再教育は，定期的に実施するべきである。

イ：新入社員に対しては，配属された各部署で業務を開始する前に実施するべきである。

ウ：全ての社員を対象として実施するべきである。

問２　【解答ウ】

バイオメトリクス認証（生体認証）は，人体固有の身体的特徴によって認証することである。認証対象者の身体的特徴をあらかじめ登録し，認証情報として識別する。したがって，バイオメトリクス認証の例として適切なものは，「本人の指紋で認証する」ことである。

問３　【解答ウ】

ア：ウイルスは，読み書きを行ったファイル以外に感染する可能性もあるので，ハードディスク全体の検査は定期的に行うべきである。

イ：ウイルスは，システムが稼働している間，いつでも侵入してくる可能性があるので，ウイルス対策ソフトは常に動作させて監視するべきである。

ウ：コンピュータウイルスは日々新種が発見されており，全てが既知のウイルスとは限らないので導入後もウイルス定義ファイルの更新を継続して行うべきである。(正解)

エ：プロバイダ側のウイルスチェックは有効であるが，USBメモリやCD-ROMなどから感染する場合もあるので，PCにもウイルス対策ソフトを導入するべきである。

問４　【解答ア】

・画像認証（CAPTCHA）
　：プログラムによる自動投稿を防止する技術である。画面に表示された歪んだ文字や数字を入力させ，人間が入力したかどうか判定する。(正解)

・コンテンツフィルタ
　：Webサイトのデータ（コンテンツ）をふるい分ける（フィルタリング）技術である。セキュリティの面や道徳的に問題のあるWebサイトなどを制限する。

・電子透かし
　：不正コピーなどを防止する技術である。画像などのデータに，通常は表示されない（透けて見える）作成日や著作権情報などを埋め込む。

・バイオメトリクス認証（生体認証）
　：人体固有の身体的特徴によって認証することである。許可されていない人間を，機器が設置されている部屋などに入れないようするために利用される。

問５　【解答ウ】

アクセス権設定は，情報資産（データベース等）へのアクセス権を利用者ごとに設定することで，不正アクセスによる情報の漏えい（②）や改ざん（④）を防ぐことを目的とする。

① 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てサービスを妨害する攻撃であり，不正侵入などを行わなくとも攻撃可能なので，アクセス権を設定しても防ぐことはできない。

③ ショルダハッキングは，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，肩越しから盗み見る行為であり，アクセス権を設定しても防ぐことはできない。

したがって，適切なアクセス権を設定することによって効果があるものは「②，④」である。

問６　【解答イ】

a：各部屋に入室を許可する社員が設定されているので，権限のある社員だけに入室を許可することができる。(適切)

b：退室は管理していないので，入室者が部屋にいた時間は記録できない。

c：入退室管理システムには全社員を登録するので，入室を試みて拒否された社員を記録することはできる。(適切)

d：退室は管理していないので，部屋にいる人数を把握することはできない。

したがって，この入退室管理システムで実現できることは「a，c」である。

問7　【解答エ】

SSL鍵マークは，データの暗号化機能とサーバ証明書による認証機能を備えたセキュリティプロトコルSSL（Security Sockets Layer）が使用されていることを表すマークである。

ア：SSLは，認証機能を備えたセキュリティプロトコルなので，サーバ証明書を確認できたことによって偽のサイトでないと判断できる。しかし，偽のサイトでないことが確認できるだけであり，ショッピングサイト運営者の財務状況が安定していることを保証するものではない。

イ：注文した商品が納品日に手元に届くかは，ショッピングサイトの運用や商品配送システムなどの問題であり，SSLで確認できることではない。

ウ：SSLでは，ディジタル署名を利用して改ざんを検出する仕組みはあるが，改ざんされた内容を修正することはできない。

エ：SSLは，データの暗号化機能を備えたセキュリティプロトコルなので，利用者などが入力した個人情報は暗号化されて送られる。その結果，途中経路で盗聴されたとしても，暗号化された内容が復号できなければ，情報が漏えいすることはない。（正解）

2．3　情報セキュリティ(5)　　アクセス制御

問1　【解答ウ】

パスワードは，利用者本人しか知らない文字列（キーワード）である。利用者が入力したIDとパスワードを使用して，システムがアクセスを許可した本人かどうか確認（利用者認証）する。パスワードの運用では，パスワードが推測されないことと，第三者に漏えいしないことに注意する。

ア：パスワードは，英数字などを組み合わせた，意味のない文字列にすべきである。英単語などを利用すると，辞書攻撃で簡単に解読されてしまう。

イ：パスワードを書いたメモなどは，人目に触れるところに置いておくべきではない。メモしたい場合には，その管理方法に十分配慮する必要がある。

ウ：パスワード漏えいの事実が明らかになった場合は，速やかに管理者に連絡すべきである。また，漏えいしたパスワードはすぐに変更するか，管理者が無効にする。（正解）

エ：パスワードは，必要十分な長さ（最低6～8文字）にすべきである。短いパスワードは，総当たり攻撃で解読されやすい。

問2　【解答ア】

・シングルサインオン
　：一度の認証で，許可されている複数のシステム（サービス，サーバ，アプリケーション）を利用できる仕組みである。（正解）
・ディジタルフォレンジックス
　：不正アクセスなどのコンピュータ犯罪が起きたとき，犯罪に関係する機器やデータを収集／分析して，法的に証拠となり得るかどうかを明らかにする技術の総称である。
・バイオメトリクス認証
　：人体固有の身体的特徴によって認証することである。許可されていない人間を，機器が設置されている部屋などに入れないようするために利用される。
・ワンタイムパスワード
　：一度しか使えないパスワード（または一度しか使えないパスワードで認証する仕組み）のことである。

問３　【解答エ】

・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。
・サーチエンジン
　：Webサービスの一つである，情報検索サイトで処理を行うプログラムである。
・スイッチングハブ
　：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。LAN内のPCから発信されたパケットは，転送する必要のないLANには伝送されない。
・ファイアウォール
　：内部ネットワークと外部ネットワークの間に設置して，通信が許可されていないパケットの侵入（不正アクセス）を防ぐ仕組みである。（正解）

問４　【解答ウ】

・DMZ（DeMilitarized Zone；非武装地帯）
　：内部ネットワークと外部ネットワークの間にファイアウォールを設置し，社外に公開するWebサーバ，メールサーバなどを社内ネットワークから隔離するためのセグメントである。ファイアウォールによって，通信が許可されていないパケットの侵入（不正アクセス）を防ぐことができる。
・IDS（Intrusion Detection System；侵入検知システム）
　：ネットワーク接続機器などへの不正侵入を検知し，ログの収集・解析を行うシスムである。あらかじめ登録してある侵入パターンに該当するアクセスパターンや，通常の運用におけるアクセスパターンと異なるものなどを検知する。
・検疫ネットワーク
　：内部ネットワークに接続するPCを，独立したネットワークにいったん接続して検査し，問題があれば対処する仕組みである。外出先で使用したPCを会社に持ち帰った際に，ウイルスに感染していないかなどを確認するために利用する。（正解）
・ファイアウォール
　：内部ネットワークと外部ネットワークの間に設置して，通信が許可されていないパケットの侵入（不正アクセス）を防ぐ仕組みである。

問５　【解答エ】

ア：一度の認証で，許可されている複数のサーバやアプリケーションなどを利用できる仕組みは，シングルサインオンである。チャレンジレスポンス認証とは，受信したチャレンジコードから一定のルールに従って求めたレスポンスコードを送信することで，一定のルールを知っている正当な利用者であることを認証する仕組みである。
イ：指紋や声紋など，身体的な特徴を利用して本人認証を行う仕組みは，バイオメトリクス認証である。
ウ：画面に表示された表の中で，自分が覚えている位置に並んでいる数字や文字をパスワードとして入力する方式は，マトリックス認証である。
エ：認証のために一度しか使えないパスワードは，ワンタイムパスワードである。ログインのたびに異なるパスワードを使用することで，外出先などで第三者にパスワードの入力を盗み見られても，そのパスワードを再利用することはできないので安全性が高い。（正解）

問６　【解答ア】

・DMZ（DeMilitarized Zone；非武装地帯）
：内部ネットワークと外部ネットワークの間にファイアウォールを設置し，内部ネットワークから隔離するネットワーク領域である。DMZには，Webサーバやメールサーバなど，社外に公開したいサーバを設置する。（正解）

・DNS（Domain Name System）
：URLやメールアドレスをIPアドレスに変換するプロトコル又は仕組みのことである。

・DoS（Denial of Service）
：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てサービスを妨害する攻撃である。

・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（又は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。

問７　【解答イ】

・ESSID（Extended SSID；ネットワーク識別子）
：無線LANのアクセスポイントを識別するネットワーク識別子である。

・MACアドレスフィルタリング
：接続を許可する端末のMACアドレス（端末固有の情報）をアクセスポイントにあらかじめ登録しておき，登録されていないMACアドレスをもつ端末からの接続を拒否する機能である。（正解）

・WEP（Wired Equivalent Privacy）
：WEPパスワードとSSIDを利用して，無線LANの暗号化を行う方式である。

・WPA（Wi-Fi Protected Access）
：WEPを改良した方式で，一定時間ごとに鍵を生成／更新する暗号化プロトコルTKIP（Temporal Key Integrity Protocol）を利用して無線LANの暗号化を行う。

2．3　情報セキュリティ(6)　暗号化／ディジタル署名

問１　【解答イ】

ア：共通鍵暗号方式は，暗号化と復号に同じ鍵（共通鍵）を使用する方式なので，暗号化に用いる鍵を第三者に公開すると，第三者は暗号文を復号できる。

イ：共通鍵暗号方式は，送信者と受信者しか鍵を知らないため，暗号化／復号の処理が簡単（少ない計算量）で，暗号通信を高速に行える。（正解）

ウ：暗号方式は，第三者に盗聴されるのを防ぐ技術であるため，改ざんされた暗号文を訂正して，元の暗号文に復元する機能はない。

エ：共通鍵暗号方式は，通信相手ごとに鍵を用意しなければいけない。

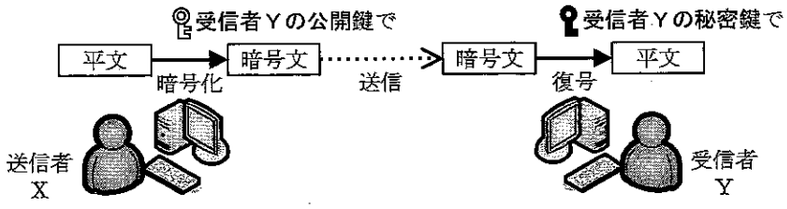
問２　【解答エ】

・AES（Advanced Encryption Standard）
　：ラインダール（Rijndael）法を利用した共通鍵暗号方式である。
・DES（Data Encryption Standard）
　：ブロック暗号を利用した共通鍵暗号方式である。
・RSA（Rivest, Shamir, Adleman）
　：非常に大きな数の素因数分解を利用した公開鍵暗号方式である。
・WPA2（Wi-Fi Protected Access 2）
　：共通鍵暗号方式（AES）を使用した，無線LANの暗号方式の規格である。（正解）

問３　【解答ウ】

公開鍵暗号方式は，暗号化の鍵を公開（公開鍵）し，復号に使う鍵を秘密（秘密鍵）にする方式である。暗号化の鍵を公開しているので暗号化の処理は複雑にしなければいけないが，一組の鍵で多数の人と暗号通信を行えるので，鍵の管理が簡単である。

図に示すように，Ｘさんが公開鍵暗号方式を用いてインターネット経由でＹさんに電子メールを送るとき，電子メールの内容を暗号化するのに使用する鍵は「Ｙさんの公開鍵」である。



問４　【解答ウ】

公開鍵基盤（PKI：Public Key Infrastructure）とは，公開鍵暗号方式やディジタル署名を利用したセキュリティ環境のことである。公開鍵基盤（PKI）でも公開鍵の正当性を確認するために，認証局（CA：Certification Authority）のディジタル証明書が利用される。したがって，公開鍵基盤（PKI）において認証局（CA）が果たす役割は，「公開鍵が被認証者のものであることを示す証明書を発行する」ことである。

ア：SSLで使用するディジタル証明書は発行するが，認証プログラムは提供しない。
イ：ディジタル証明書でWebサーバの認証はできるが，不正な仕組みがないことは示せない。
エ：ディジタル署名を送信するのは，ディジタル署名を作成した送信者である。

問５　【解答ウ】

ア：二重に暗号化するのではなく，共通鍵を公開鍵で暗号化する。
イ：暗号通信は，共通鍵を使用した共通鍵暗号方式で高速に行える。
ウ：セション鍵暗号方式で用いられるハイブリッド方式では，暗号通信を行うための共通鍵を生成し，その共通鍵を通信相手の公開鍵で暗号化して送信する。その後は共通鍵を利用した共通鍵暗号方式で，暗号通信を高速に行う方式である。（正解）
エ：ｎ人で暗号通信を行う場合，共通鍵暗号方式では$n(n-1)$個，公開鍵暗号方式では$2n$個の鍵が必要となる。ハイブリッド方式では共通鍵を生成するので，使用する鍵の数を，管理する鍵の数と考えれば公開鍵暗号方式と同じ$2n$個，共通鍵を含めても$2n+n(n-1)=n^2+n=n(n+1)$個となり，どちらにしても２乗倍になることはない。

問６　【解答エ】

ａ：ウイルスに感染していないかは，ウイルス対策ソフトで確認する。
ｂ：盗聴を防止するためには，共通鍵暗号方式や公開鍵暗号方式で暗号化する。
ｃ：ディジタル署名では，暗号化されたハッシュ値を送信者の公開鍵で復号することで，対応する秘密鍵を知っている本人であることを確認し，なりすましを判断できる。
ｄ：ディジタル署名では，受信したハッシュ値と，受信した平文から算出したハッシュ値を比較することで，改ざんの有無について判断できる。
したがって，ディジタル署名を付与した場合は「ｃ，ｄ」について判断可能である。

問７　【解答エ】

暗号化の手順を逆にして，暗号化した結果を復号する。
手順１　暗号化した結果“tmb”を数値に変換する。
tmb　→　't', 'm', 'b'　→　20, 13, 2
手順２　各文字を表す数値から，１文字目なら１，２文字目なら２，３文字目なら３を引く。この減算で計算結果が０以下になった場合は，26を加算して１～26の範囲に調整する。
１文字目't'：　20 － 1 ＝ 19
２文字目'm'：　13 － 2 ＝ 11
３文字目'b'：　2 － 3 ＝ －1
→　０以下になったので26を加算：　－1 ＋ 26 ＝ 25
手順３　求めた数値を英字に変換する。
19, 11, 25　→　's', 'k', 'y'　→　元の文字列「sky」

２．４　マルチメディアとヒューマンインタフェース(1)　マルチメディア技術

問１　【解答ウ】

Webコンテンツを，文字情報のリンクによって関連付けるハイパーテキストに対し，ハイパーメディアは，画像などのリンクによって結びつけるマルチメディアコンテンツに付けられた名称である。つまり，「文字情報だけでなく，画像情報などにもリンクが設定できるコンテンツである。」
ア：Webコンテンツに関する説明である。
イ：マルチメディアコンテンツに関する説明である。
エ：ハイパーテキストに関する説明である。

問２　【解答ウ】

・アーカイバ
：複数のファイルを一つにまとめたり，元に戻したりするソフトウェアである。
・アンチエイリアシング
：斜線や曲線に生じるギザギザを目立たなくするコンピュータグラフィックスの技術である。
・オーサリング（マルチメディアオーサリングツール）
：文字や図形，静止画像，動画像，音声など複数の素材を組み合わせて編集し，マルチメディアコンテンツを作成するソフトウェアである。（正解）
・プラグイン（プラグインソフトウェア）
：別のソフトウェアに組み込むことで，機能を拡張するソフトウェアである。

問３　【解答イ】

ア：一般的には，元のデータに完全に復元できるだけのデータが必要となる可逆圧縮方式で圧縮するほうが，非可逆圧縮方式で圧縮するより圧縮後のデータのサイズは大きくなる。

イ：可逆圧縮方式では圧縮したデータから元のデータに完全に復元できるが，非可逆圧縮方式では元のデータに完全に復元できない。ただし，復元が多少不完全でも，人間には違いがほとんどわからないため，大きな問題になることはない。（正解）

ウ：可逆圧縮方式では元のデータに完全に復元するために固定の圧縮率を使用するが，非可逆圧縮方式では復元した際の粗さに応じて圧縮率を調整できる。

エ：可逆圧縮方式／非可逆圧縮方式は，復元されるデータの違いによる分類であり，どちらの方式も圧縮／伸張が行える方式である。

問４　【解答イ】

DRM（Digital Rights Management；ディジタル著作権管理）は，ディジタルデータとして表現された映画，音楽，小説などのコンテンツの著作権を保護し，利用や複製を制限する技術の総称である。

ア：MPEG（Moving Picture Experts Group）に関する説明である。

ウ：BML（Broadcast Markup Language）に関する説明である。

エ：ドルビーディジタルに関する説明である。

問５　【解答エ】

ストリーミングは，映像や音楽のデータをダウンロードしながら再生する技術である。従来のように，完全にダウンロードし終わってからでないと再生できない方式では時間がかかり過ぎるため，ダウンロードと再生を並行して行うストリーミングが考え出された。

ア：ストリーミングでは，イベントやスポーツなどを撮影しながら配信（ライブ配信）することも可能である。

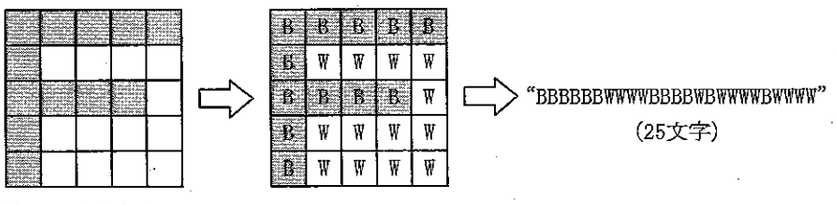
イ：ストリーミングは，データの完全性よりもリアルタイム性を優先しているので，受信データの部分的な欠落による画質の悪化を完全に排除することはできない。

ウ：動画再生の際には，一定量のデータを読み込んで蓄積（バッファリング）する必要がある。

問６　【解答イ】

圧縮しない表現と圧縮した表現を求めてから，圧縮率を計算する。

手順１　圧縮しない表現を求める。



手順２　圧縮した表現を求める。

圧縮しない表現：“BBBBBB WWWW BBBB W B WWWW B WWWW”

圧縮した表現　：“ B6　W4　B4　W B　W4　B　W4 ”（13文字）

手順３　圧縮率を求める。

圧縮率＝圧縮した表現の文字数÷圧縮しない表現の文字数

＝13文字÷25文字

＝0.52　→　「52.0」％