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。

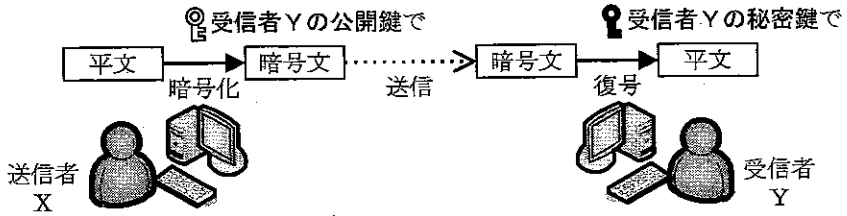
問２　【解答エ】

・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。