セキュリティ演習解説

問１　ウ

セキュリティポリシに関する問題である。

安全の保障を可能にするためには、セキュリティに関するマネジメントの方針を設定することが重要である。セキュリティマネジメントとは、安全を組織的に計画し、実施し、その結果を計量評価し、次期の計画に反映させることである。

セキュリティ方針には、次の内容を盛り込む必要がある。

①　情報は組織体における貴重な資産　　②　情報の漏洩、改変、破壊の防止

③　作為、不作為に関係しない。　　④　効果的かつ経済的保護

⑤　組織体構成員全員の義務

企業の情報セキュリティポリシは企業の考え方や取り組み方を明文化することであり、求める答えはウとなる。

問２　ウ

データの破壊や可用性が損ねた場合の損失費用の問題である。

データの破壊やシステムの可用性が損なわれた場合に発生する損失費用であるから、破壊したシステムが復旧するまでの間、代替の手段に費やした費用になる。求める答えはウとなる。

アは業務形態の変更に伴うシステムの再開発に必要な費用になる。

イはシステム計画時の実現可能性の検討にかかる費用である。

エはシステム開発後に新しいシステムに移行するために発生する費用である。

問３　ア

情報セキュリティの完全性に関する問題である。

完全性はネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないことである。完全性の喪失は、通信路上のデータ、ハードディスク内のデータ、フロッピーディスク内のデータの改ざんや破壊が行われたり、インターネット上の電子商取引において、金額情報の改ざんが行われたりすることである。長時間かけて蓄積、作成した情報源が破壊されると、その復旧に膨大な時間と金を必要としたり、時には復旧不能にもなる。交通システムに侵入され、制御情報を改ざんされると、生命の危険が生じかねない。

アは完全性、イ、エは機密性、ウは可用性である。求める答えはアとなる。

問４　ア

コンピュータセキュリティ対策に関する問題である。

アの記憶領域に残っている機密データはジョブ終了時に確実に消去することはセキュリティ対策として重要である。求める答えはアとなる。

イのデータにチェックディジットを付加することは入力データのチェックには役立つがサラミ技術などの犯罪の防止対策にはならない。

ウの内容の仮想記憶領域のページまたはセグメント単位に割り付けられた記憶保護キーの保護

レベルの変更は、データの改ざんは実記憶域の主記憶で行われるためセキュリティ対策にはならない。

エの内容のユーティリティプログラムのバックアップをとっておき、元のプログラムとの変化が分かっても、データの改ざんを防止できることにはならない。

問５　エ

インターネットのＶＰＮに関する問題である。

ＶＰＮは、インターネットを専用線のように利用したネットワークで、通常の専用線と比較して、通信コストが安くなる。認証システムや暗号技術、トンネリング、ファイアウォールなどを利用することで、インターネット上を流れるデータを保護する。組織外のユーザがネットワーク上を流れるデータにはアクセスできない。トンネリングは、インターネットなどの公衆回線網上に、ある２点間を結ぶ閉じられた仮想的な直結通信回線を確立することであり、ネットワーク上に外部から遮断された見えない通り道を作るように見えることからトンネルと呼ばれるようになった。本来通信を行ないたいプロトコルで記述されたパケットを、別のプロトコルのパケットでカプセル化して、送り届けることにより通信を行なう。パケットのカプセル化とその解除はトンネルの両端の機器が自動的に行なうため、トンネルで結ばれた機器同士は途中の通信方式や経路を気にする必要はなく、あたかもトンネルの両端の機器が直結しているように見える。本社と支社のＬＡＮ間接続など、プライベートなネットワークをインターネットを経由して接続する際などに利用されることが多いため、実際のトンネリング機器やソフトウェアはパケットをカプセル化する際に暗号化を行ない、転送中に覗き見られたり改ざんされたりしないようにするセキュリティ機能を持っていることが多い。

アは、暗号技術と認証システムを活用して専用化を行っているので、暗号技術は不可欠である。

イは、盗聴防止の機能はなくてもが、暗号化によってデータの解読が不能になるため、データの内容は保護されることになる。

ウは、暗号技術と認証システムを使用しているため、第三者による盗聴や改ざんは防止できる。

エのネットワークに参加する資格の区別は組織単位であって、通常は、個人を識別する能力はない。求める答えはエとなる。

問６　エ

電子メールの添付ファイルの処理に関する問題である。

コンピュータウィルスは第三者のコンピュータシステムに侵入して正常な動作を妨げることを目的として作成されたプログラムである。電子メールの添付ファイルを開くだけで感染することがある。不審なメールは開かない、添付ファイルは自動的に開く設定にしないなどの対策が必要である。

アの履歴不明の添付ファイルを開くことは問題である。適切な動作ではない。

イの送信先にフィルを開くことを依頼するのも問題がある。開くと感染する可能性がある。

ウの現状問題がないという理由で、そのまま放置するのも問題である。ある時期に発病する可能性がある。

エの添付ファイルを開かないように連絡し、セキュリティ担当者に調査を依頼するのが適切である。求める答えはエとなる。

問７　イ

コンピュータウィルス対策に関する問題である。

アの感染直後の一般利用者のウィルスの種別の解明は、対象の種類が多く登録されていない新種のウィルスもあり、簡単にはできない作業である。最初の作業としては正しくない。

イの感染媒体の破棄、ワクチンによるウィルスの除去の試みは正しい。ただし、ウィルスが除去できるとは限らないため、その場合には媒体の破棄になる。求める答えはイとなる。

ウの最新バージョンのワクチンを使用しても、ウィルスの感染を完全に除去することは困難である。

エのバックアップファイルへのウィルス感染の防止は、バックアップファイルに感染データやプログラムなどを書き込まなければよいから、ライトプロテクトで十分である。

問８　ウ

電子メールの宛先アドレス確認に関する問題である。

アのＯＰ２５Ｂは、ネットワークの境界にあるルータなどの機器で、ネットワーク内から外部のコンピュータのＴＣＰポート25番への通信を禁止することである。これによって、電子メールが送信不能になる。

イのＳＰＦは、メールの送信元アドレスの偽装を防止する技術である。ドメインと無関係なメールサーバを利用して送信元を偽ったメールを送信しようとすると、受信側でそのことを検出して自動的に受け取りを拒否することができる。

ウの誤送信対策としては、電子メールの送信者が送信時に、宛先アドレスの確認を行うことは有効である。求める答えはウとなる。

エの不正中継は、メールサーバを運用しているサイトで受け取り先のサーバとは全く関係のないメールが第三者によって送り付けられ、これを受け取ったサーバが本来必要のないメール配送処理をさせられてしまう現象である。 送信者に宛先アドレスの確認を求めても意味がない。

問９　イ

コンピュータウィルス対策基準の３つの機能の組み合わせに関する問題である。

コンピュータウィルスの３つの機能は次の内容である。

① 自己伝染機能：自らの機能によって他のプログラムに自らのプログラムをコピーし、またはシステム機能を利用して自らのプログラムを他のシステムにコピーすることにより、他のシステムに伝染する機能。

② 潜伏機能：発病するための特定時刻や一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能。

③ 発病機能：プログラムやデータ等のファイルの破壊を行ったり、設計者の意図しない動作をするなどの機能。

コンピュータウィルス対策基準で定義されている３機能は、自己伝染機能、潜伏機能、発病機能であり、求める答えはイである。

問10　エ

コンピュータウィルスに関する問題である。

ウィルスにはシステム感染型とファイル感染型がある。システム感染型はフロッピーディスクを介してハードディスクのブートセクタに感染し、システムを起動するたびにメモリに読み込まれてしまうタイプである。ファイル感染型はプログラムファイルに感染し、感染プログラムを起動するとメモリに読み込まれるタイプである。

アのファイルの起動と感染の関係では、一定の潜伏期間を経過すると発病するものもあり、ファイルが起動されなければ感染しないとは言えない。

イのウィルスは主記憶を物理的に破壊することはない。物理的に破壊するは誤りである。

ウの新しいワクチンでも有効でないウィルスが存在する。

エの感染していないＯＳの起動ディスクを使用すると、ブートセクタからの感染は防止することができる。求める答えはエとなる。

問11　ウ

ワームに関する問題である。

ワームはコンピュータウィルスの一種で、ネットワークを感染経路にして自己増殖し、システムに害を与える悪質なコンピュータプログラムである。ワーム自体は破壊を行わないが、増殖を繰り返していくことでコンピュータのＣＰＵの処理やディスクの容量などを占有し、システムに負荷をかけたり、停止させたりする。

ウのネットワーク経由でコンピュータ間を自己複製しながら移動するが適切な記述である。求める答えはウとなる。

アはマクロウィルス、イは時限爆弾や論理爆弾、エは狭義のウィルスであり、ファイル感染型やカーネル感染型が相当する。

問12　ウ

コンピュータウィルス対策に関する問題である。

コンピュータウイルスは感染する場所によって大別できる。プログラムファイルに感染するものをプログラムファイル感染型、ハードディスクの起動を管理する部分に感染するものをブートセクター感染型、アプリケーションが持つマクロ機能を悪用しデータファイルに感染するものをマクロ感染型と呼ぶ。プログラムファイルとブートセクターのどちらにも感染する複合感染型もある。特に最近は電子メールの普及でデータファイルをやり取りする機会が増え、マクロ感染型による被害が急増している。ウイルスの感染経路は電子メールを使ったファイルのやり取りが大半を占める。添付ファイルを開くことによって感染し、さらに感染したパソコンのアドレス帳を読み出して、勝手にウイルスに感染したファイルを電子メールで送るものも多い。インターネットなどからダウンロードしたプログラムやフロッピーディスクなどのリムーバブルメディアの受け渡しの場合もある。感染予防としては、ウイルスの発見や駆除を行うウイルス対策ソフトが不可欠である。また、ダウンロードしたファイルや電子メールの添付ファイルは開く前にこまめにチェックする、外部から持ち込んだハードディスクなどは初期化してから使う、不特定多数の人とのハードウエアやフロッピーディスクの共用を避けるといった注意も必要である。

アの論理フォーマットではウィルスを消去することが出来ない。

イは書き込み禁止処理を行ってからインストールする方が好ましい取扱である。

ウのソフトウェアをインストールする場合はコンピュータ自身がウィルスに感染していないか

どうかを確認してから実行する記述は適切な内容である。求める答えはウとなる。

エのウィルス対策は管理責任者を設置して講じるべきである。

問13　イ

ウィルス定義ファイルに関する問題である。

ウィルス定義ファイルは、コンピュータウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録したファイルで、ワクチンソフトがコンピュータウイルスやワームを検出するのに使う。「パターンファイル」などとも呼ばれる。ワクチンソフトはウイルス定義ファイル内に収録された各ウイルスのパターンと検査対象のファイルを照合し、パターンとの一致が見られるとそのファイルがウイルスに感染していると判断する。次々と現れる新種のウイルスに対応するため、各ワクチンソフトメーカーは頻繁に自社ソフト向けの新しいウイルス定義ファイルをインターネットなどで配布している。

アの修復するためのファイルではなく、検出するためのファイルである。

イの記述内容が適切である。求める答えはイとなる。

ウのウィルスを再現し、動作を監視するために使用するは誤りである。

エの復旧のためのファイルは誤りである。

問14　ア

ウィルスの調査法に関する問題である。

アのバイナリファイルを逆アセンブルしてアセンブラ言語のプログラムにすることはウイルスの動作を解明に有効である。求める答えはアとなる。

イのパターンマッチングは既知のウイルスやその亜種の検出に効な手法である。

ウのファイルのハッシュ値を確認することでウイルスに感染しているかどうかを確認することができる。

エの不正な動作からウイルスを検知する方式は、振る舞いから未知のウイルスを検出することが可能である。ビヘイビア法は検査対象のプログラムを実行してその振る舞いを監視するウイルス検出方法の1つであり、ウイルス対策ソフトの既知のウイルスパターンに存在しない未知のウイルスを検出するために用いられる。

問15　エ

コンピュータウィルスに関する問題である。

アのサラミ法は、多数の資源からわずかの資産をさく取するウィルスの１種である。預金システムの利息の端数処理プログラムを操作して、切り捨て額を犯人の口座に振り込ませる犯罪に用いる。

イのスーパザップ法は、緊急事態に対処するためにシステムが備えている、あらゆる資源を回避してプログラムやファイルにアクセスして変更できるようにする機能を悪用する。

ウのタッピングは、ネットワーク上の電文を不正に盗み取る行為である。

エのトロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、不正行為を実行させる仕組みのウィルスの１種である。求める答えはエとなる。

問16　ウ

コンピュータウィルス対策に関する問題である。

ウィルス対策の８箇条

①　最新のワクチンソフトを活用すること

②　ウィルス対策に備えてデータのバックアップを行うこと

③　ウィルス感染の可能性が考えられる場合、ウィルス検査を行うこと

④　コンピュータウィルスを発見した場合、感染したコンピュータをネットワークから直ちに切り離す。

⑤　メールの添付ファイルはウィルス検査後開くこと

⑥　ウィルス感染の可能性のあるファイルを扱うときは、マクロ機能の実行は行わないこと

⑦　外部から持ち込まれたフロッピーディスクおよびダウンロードしたファイルはウィルス検査後使用すること

⑧　コンピュータの共同利用時の管理を徹底すること

アの処理は、感染したコンピュータをネットワークから切り離し後、行う。

イのオンライン状態のままでは、他のコンピュータに感染する危険性がある。

ウのネットワークからの切り離しは直ちに行う処置であり、適切である。求める答えはウとなる。

エのコンピュータの電源を切っても、ウィルスの除去にはならない。

問17　ウ

コンピュータウィルスに関する問題である。

アのＤｏＳ攻撃は、サーバなどのネットワークを構成する機器に対して攻撃を行い、サービスの提供を不能な状態にすることである

イの辞書攻撃は、クラッカーが特定のコンピュータに施されたパスワードを調べたり、スパム送信者が送信先のメールアドレスを決める際に用いる手法である。

ウのトロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、データの破壊、改ざんなどの不正行為を実行させるウィルスである。求める答えはウとなる。

エはバッファー領域をオーバフローさせる攻撃である。

問18　イ

フィッシングに関する問題である。

アのＤＤｏＳ攻撃は、第三者のマシンに攻撃プログラムを仕掛けて踏み台にし、その踏み台とした多数のマシンから標的とするマシンに大量のパケットを同時に送信する攻撃である。

イのフィッシングは、金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺の一種である。求める答えはイとなる。

ウのポットは、ハニーポットといい、ハッカーやクラッカーに対して、あたかも“本物のシステム”であるかのように見せかけるおとりのような仕組みである。

エのメールヘッダインジェクションは、問い合わせフォームなどのメールを送信する画面で、メールの内容を改ざんし、迷惑メールの送信などに悪用する脆弱性である。

問19　イ

ソーシャルエンジニアリングに関する問題である。

ソーシャルエンジニアリングは、ネットワークシステムへの不正侵入を達成するために、必要なＩＤやパスワードを、物理的手段によって獲得する行為を指す。代表的な例として、侵入した企業・組織の従業員になりすましてパスワードを聞き出したり、盗み聞きしたりする行為が挙げられる。ほかにも廃棄された紙ゴミから企業・組織に関する重要情報を読み取るなどの行為もあり、電話に出た子どもに対して、両親に関する個人情報を聞き出す事例などがある。

システム管理者などを装い、利用者に問い合わせてパスワードを取得する行為はソーシャルエンジニアリングである。求める答えはイとなる。

アはバックドア、イはソーシャルエンジニアリング、ウはフルートフォース攻撃、エはセキュリティフォールである。

問20　エ

フィッシングに関する問題である。

フィッシングは、金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺の一種である。

アはクロスサイトスクリプティング、イはマルウェア、ウはスパイウェア、エはフィッシングである。求める答えはエとなる。

問21　エ

ウィルスの予防対策に用いられるワクチンに関する問題である。

アのクリッパーは記憶容量を食いつぶすウィルスである。

イのカスケードは画面の表示文字を下方に落とすウィルスである。

ウのミケランジェロはミケランジェロの誕生日に初期化するウィルスである。

エのワクチンはウィルスの検出・駆除対策に利用される。求める答えはエとなる。

問22　ア

コンピュータ犯罪の手口に関する問題である。

アのサラミ法は、コンピュータ犯罪の手口の一つて、システム開発担当のプログラマが、利子の金額を計算する際に切り捨てられる端数(日本なら1円未満の金額)を特定の休眠口座に集めるようにプログラムを細工しておき、ある程度金額がまとまった時点で自分の口座に移し換えて詐取する方法である。サラミを少しずつ切り取る様子に例えて、この名前が付けられた。

イのスキャピンジングは、プログラム実行後のコンピュータ内部に残っている情報やデータを密かに入手して悪用する手段である。

ウの盗聴は、ネットワークを介して送受信しているデータを不正に傍受することで、クレジット・カード番号や銀行口座番号など金銭に関係する情報、コンピュータ・システムへのログインに必要なIDとパスワードなどの情報が盗聴の対象となることが多い。

エのトロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、データの破壊、改ざんなどの不正行為を実行させるウィルスで、ファイルを削除してしまう機能を持ったプログラムを作る。利用者がプログラムを起動すると、ファイルが勝

手に削除されてしまう。

アはサラミ法、イは盗聴、ウはトロイの木馬、エはスキャビンジングの内容を示している。求める答えはアとなる。

問23　ウ

サラミ法に関する問題である。

サラミ法は、多数の資源からわずかずつ資産を搾取する方法である。預金システムの利息の端数処理プログラムを操作して、切り捨て額を犯人の口座に振り込ませる。プログラムの操作にはトロイの木馬を応用する。

アはなりすまし、イは盗聴、ウはサラミ法、エはスカビンジングである。求める答えはウとなる。

問24　ウ

マクロウィルスに関する問題である。

マクロウィルスは表計算やワープロなどのマクロ言語で記述された文書データに潜み、電子メールを介して送信相手に感染するタイプのコンピュータウィルスである。マクロウィルスの１種であるメリッサは、感染した電子メールを受け取ったユーザが、メールに添付されたワード文書を開き、自動的にマクロが実行されると直ちに感染し、同時に発病する。求める答えはウとなる。

アはファイル感染型、イはブートセクタ感染型であり、マクロウィルスではない。

エの感染が容易に判断できるは誤りであり、文書を開き、マクロを実行した段階で発病するため通常の手段では簡単に把握することができない。

問25　ウ

ペネスレーションテストに関する問題である。

ペネスレーションテストは、ネットワーク接続された情報システムが外部からの攻撃に対して安全かどうか、実際に攻撃手法を試しながら安全性の検証を行う。不正に侵入できるかどうかだけでなく、ＤｏＳ攻撃にどれくらい耐えられるかを調べたり、侵入された際にそこを踏み台にして他のネットワークを攻撃できるかどうかなどを調べる場合もある。

アのウォークスルー、イのソフトウェアインスペクションはシステム開発でのデザインレビューの方法の一つである。

ウのペネストレーションテストは、コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで、システムを実際に攻撃して侵入を試みる手法である。求める答えはウとなる。

エのリグレッションテストは、情報システムの一部に修正を加えたときに、修正部分が他に悪影響を与えてないかどうかを確認するテストである。

問26　イ

コンピュータウィルス対策ソフトに関する問題である。

ウィルス対策ソフトはコンピュータウィルスを発見するために使用されるファイルである。パターンファイルに蓄積されているウィルスの情報を利用してファイルをチェックする。パターン

ファイルにないウィルスは発見できない可能性が高い。ウィルスに感染しないためにはパターンファイルを常に最新の状態にしておく必要がある。

アの感染前後のファイルを比較しても変化は分かるがウィルスに感染したかどうかを判断することはできない。パターンファイルとの比較が必要である。

イの既存ウィルスのシグネチャコードと比較するとウィルスを検出できる。求める答はイとなる。

ウのウィルスに起因する異常現象を絶えず監視することができない。新しいウィルスによる異常現象を特定する事ができない。

エのファイルとの照合はパターンファイルと行うのであって、チェックサムと照合してもウィルスを検出することはできない。

問27　ア

ＳＱＬインジェクションに関する問題である。

ＳＱＬインジェクションは、Ｗｅｂサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてＳＱＬ文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃である。

Ｗｅｂアプリケーションではデータベースの操作にＳＱＬ言語を利用している。ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。このとき、ＳＱＬ文として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり、本来アクセスできない情報を表示させたりすることができてしまう場合がある。

アはＳＱＬインジェクション、イはクロスサイトリクエストフォージェリ、ウはワームの一種のＳＱＬ Slammer、エはクロスサイトスクリプティングである。求める答えはアとなる。

問28　ア

ＳＱＬインジェクション攻撃に関する問題である。

ＳＱＬインジェクションは、Ｗｅｂサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてＳＱＬ文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃である。

Ｗｅｂアプリケーションではデータベースの操作にＳＱＬ言語を利用している。ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。このとき、ＳＱＬ文として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり、本来アクセスできない情報を表示させたりすることができてしまう場合がある。

開発・導入したＷｅｂアプリケーション、またはデータベース上のストアドプロシージャ等を改修し、意図しないＳＱＬ文を受け入れないようにする必要がある。即ち、入力中の文字がデータベースへの問合せや操作において、特別な意味をもつ文字として解釈されないようにする必要がある。求める答えはアとなる。

問29　ア

ソーシャルエンジニアリングに関する問題である。

アのソーシャルエンジニアリングは技術的な手段によらずに巧みな話術やゴミ箱を漁るといった方法で顧客や従業員のパスワードや機密情報などを不正に取得する行為をいう。求める答はアとなる。

イのトロイの木馬はプログラムコードの中に、本来の処理に影響を与えないように未承認のコードを隠しておき、不正行為を実行させる。コンピュータの全ファイルを破壊したり、パスワードを盗み出したりする。

ウのパスワードクラックは他人のパスワードを解析し、探り当てることである。人名や誕生日、意味のある単語をパスワードに使うのは避け、数字や記号を混在させることで、被害に遭う可能性を減らすことができる。

エの踏み台攻撃はセキュリティ対策の甘いサイトに不正侵入し、他サイトの攻撃の中継サイトとして利用することである。

問30　イ

ディレクトリトラバーサル攻撃に関する問題である。

ディレクトリトラバーサルは、ネットワーク上の脆弱性を利用した攻撃手法の一種で、「../」を利用してディレクトリを遡り、本来はアクセスが禁止されているディレクトリにアクセスする手法のことである。または、そのような脆弱性のことである。ネットワーク上でディレクトリのパスを指定する際、「一つ上の階層へ上る」ことを指示する「../」のパスを組み合わせて指定することで、公開されているディレクトリの上階層から、その併置されている非公開のディレクトリへアクセスできてしまう場合がある。このような操作によって、個人情報や機密情報を盗まれたり、悪意あるコードを書き込まれたりといった被害を被る危険性が生じる。

アはＳＱＬインジェクション、イはディレクトリトラバーサル攻撃、ウはクロスサイトスクリプティング、エはセションハイジャックである。求める答えはイとなる。

問31　イ

ＤＮＳキャッシュポイズニング攻撃に関する問題である。

ＤＮＳはドメイン名とＩＰアドレスの対応を検索するサーバであるが、この処理を効率化するためにキャッシュを利用する。過去に行った内容と同じ問い合わせをする場合、他のネームサーバへ問い合わせることなく、キャッシュとして保持している情報を利用してクライアントに返答する。

ＤＮＳキャッシュポイズニング攻撃は、ＤＮＳのこの機能を悪用し、キャッシュサーバに偽のＤＮＳ情報をキャッシュとして蓄積させ、攻撃を受けたキャッシュサーバを利用するユーザーに対して、以下のような影響を与える。

①　ホスト名とＩＰアドレスの対応を変更し有害サイトへ誘導する。

②　Ｗｅｂメールの内容を盗聴する、改ざんする。

③　ｓｐａｍを送信する。

⑤　ＤＮＳを使用不能にして、各種サービスやアプリケーションを動作不能にする。

アはポストスキャン、イはＤＮＳキャッシュポイズニング、ウはＤＮＳリフレクション、エは

ゾーン転送を悪用した登録情報の収集である。求める答えはイとなる。

問32　エ

情報漏洩に関する問題である。

情報漏洩は、内部の機密情報などが外部に漏れてしまうことである。パソコンなどに情報を保存し、情報漏洩対策を怠ると漏洩する恐れがある。漏洩の原因となるのは、スパイウェアなどのインストール、クラッキング、パソコンや記憶媒体などの紛失、電子メールの一斉送信がある。

アのチェックサムは誤りの検出機能、イのミラーリングは信頼性向上、ウの遠隔地保管はバックアップ機能、エの暗号化は漏洩対策である。求める答えはエとなる。

問33　エ

電子計算機使用詐欺罪に関する問題である。

アは通常の詐欺罪である。計算機と関係ない犯罪にも適用される。

イの電磁的記録不正作出罪は人の事務処理を誤らせる目的で、権利、義務、または事実証明に関する電磁的記録を不正に作出した者は処罰されることになっている。

ウの電子計算機損壊等業務妨害罪は、コンピュータの損壊や動作障害などコンピュータ業務を妨害した者は処罰される。

エの電子計算機使用詐欺罪は虚偽のデータや不正のプログラムなどを入力して、自分の預金口座に振り込み入金をさせたり、偽造や変造したプリペイドカードを使って不正な利益を得る行為などを詐欺罪として処罰する。求める答えはエとなる。

問34　ウ

リスクアセスメントに関する問題である。

リスクアセスメントは、リスク特定、リスク分析、リスク評価を網羅するプロセスである。

① リスク特定　リスクを発見し、認識し、記述するプロセス

② リスク分析　リスクの特質を理解し、リスクレベルを決定するプロセス

③ リスク評価　リスクとその大きさが受容可能かを決定するためにリスク分析の結果をリスク基準と比較するプロセス

安全工学上は、リスクとは、人、環境、物に悪い影響をあたえる可能性と大きさ(の積)である。予測されるリスクの可能性と大きさ(予測値)と、許容されるリスクの可能性と大きさ(許容値)を比較し、予想値が許容値を上回った時リスク軽減の施策又はリスク回避の施策をとるという意思決定を行い、実際にその施策をとり、より安全な状態を実現するプロセスである。

アのリスクアセスメントは、わかっている現状のレベルでの分析、評価が必要で、それに基づいて将来のリスクを予測するプロセスを繰り返す必要がある。

イの過去のリスクアセスメントの利用は不可欠である。

ウの損失額と発生確率の予測に基づいて、対応の優先順位を付けるは適切である。求める答えはウとなる。

エのリスクが顕在化してからの分析、予測、評価は価値がない。

問35　ア

リスク分析に関する問題である。

リスク分析は､情報システムを利用することに伴って発生する可能性のあるリスクを洗い出し､その影響度合いを分析することである。

リスク分析の手順

①　発生が予想されるリスクを明確にする。

②　リスクの発生頻度と１回の発生ごとの損失額を推定し、それを基に年間の損失額を算出する。

③　リスクの発生機会を減らす対策と１回当たりの損失額を減らす対策の両面から、具体的リスク対策を策定する。

④　リスク対策を実施する。

アの損失額と発生確率を予測し､リスクの大きさに従って優先順位を付ける記述は適切である。求める答えはアとなる。

イは､リスクは人間の欲望の変化や技術の変化､産業組織の変化などによって絶えず変動する。従って、リスク対策のすべてが完了しないうちにも、絶えずリスク分析を繰り返す必要がある。

ウの過去の類似プロジェクトのデータを分析に活用する。

エのリスク分析の目的は、リスクによる損失額を知ることではなく、リスクによって発生する損失を減らすことが目的である。

問36　イ

リスクの移転に関する問題である。

リスク移転はリスクコントロールの手法の一つであり、リスクの発生時の責任を契約書などで他社に転嫁することである。従って、保険に加入するなど資金面での対策を講じることになる。リスクコントロールの手法には、リスク回避、リスク分離、リスク結合、損失予防、損失軽減等がある。

アは損失予防、イはリスク移転、ウはリスク回避、エはリスク分離やリスク結合である。求める答えはイとなる。

問37　エ

リスクコントロールに関する問題である。

アのリスク移転は、特定のリスクに関する損失の負担を他者と分担することである。

イのリスク回避は、リスクのある状況に巻き込まれないようにする意思決定又はリスクのある状況から撤退する行動である。

ウのリスク低減は、特定のリスクに関する確からしさもしくは発生確率､好ましくない結果又はその両者を低減する行為である。

エのリスク保有は、特定のリスクに関する損失の負担を享受することである。求める答えはエとなる。

問38　ア

ＬＡＮアナライザの運用上の注意点に関する問題である。

ＬＡＮアナライザは、ＬＡＮの故障診断、監視、問題解決などに使用する機器やソフトウェアである。パケットの衝突率、ネットワークのトラフィックの測定、各種プロトコルの解析したりする。また、ネットワークを通過するパケットを表示できるものがあるため、盗聴などに悪用されることがある。求める答えはアとなる。

問39　イ

緊急事態計画に関する問題である。

緊急事態計画は火災や地震などの災害発生時や大事故や大事件などの緊急事態に備えて、業務をどのように継続するか、システムをいかに早く復旧するかを定めた計画書である。

アは、仕組みを考えるプログラマとその仕組みを操作するオペレータを分離しておくことによってセキュリティの予防となる。

イの緊急事態計画は、災害発生時の復旧対策であり、復旧である。求める答えはイとなる。

ウのパスワードの利用は不正アクセスの検知である。

エのメッセージ認証はメッセージ改ざんの検知である。

問40　ウ

バックドアに関する問題である。

アのシンクライアントエージェントは、機能を絞ったクライアント用コンピュータのことで、サーバ側でアプリケーションソフトやファイルなどの資源を管理するシステムである。

イのストリクトルーティングは、送信元からあて先までに経由するルーターのＩＰアドレス・リストを，送信元のルーターがすべて指定し，その順番通りにパケットを送信することである。

ウのバックドアは、ＩＤやパスワードを使って通信を制限したり、使用権を確認するコンピュータの機能を無許可で利用するために、コンピュータ内に設けられた通信接続の機能を指す。バックドアには、設計・開発段階で盛り込まれるものや稼動中のコンピュータに存在するセキュリティホールを使って送り込まれたソフトウェアである。求める答えはウである。

エのフォレンジックは、証拠として使えるように，コンピュータ内やネットワーク上にあるディジタル・データを収集・分析・保存することである。

問41　ウ

ネットワークシステムのセキュリティ対策に関する問題である。

アのコールバックは、公衆回線を利用した通信で、接続要求側が接続先を呼び出し、回線を一端切断した後に接続先が接続要求側に折り返し接続して、通信回線を開く方法である。

イの回線暗号化装置の設置は暗号化アルゴリズムを使用して通信文を暗号文に変換するだけであり、通信上のハードウェアやソフトウェアの変更を必要としない。

ウの閉域接続機能をもつ回線交換網は外部からの不正アクセス防止に有効である。求める答えはウとなる。

エの無線ＬＡＮも盗聴される。

問42　エ

コンテンツの改ざんが発生した場合の処理手順の問題である。

通常、次の手順で行う。

① 問題が発生した箇所、サーバをネットワークから切り離す。

② 問題内容をログを使用して分析し、不正アクセスの手法、影響範囲、進入経路を特定する。

③ システムを再構築する。

④ ネットワークに接続し、監視する。

答えは、③→①→②→④となり、求める答えはエとなる。

問43 ア

ＷＡＦに関する問題である。

ＷＡＦは、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。ＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

外部ネットワークからの不正アクセスを防ぐためのソフトウェアあるいはハードウェアである。ファイアウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことである。

Ｗｅｂサーバおよびアプリケーションに起因する脆弱性への攻撃を遮断する内容が適切である。求める答えはアとなる。

問44 イ

ＷＡＦに関する問題である。

ＷＡＦの特徴は、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。ＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

アのＳＳＬ-ＶＰＮは、暗号化にＳＳＬを利用するＶＰＮ技術で、多くのＷｅｂブラウザやメールソフトは標準でＳＳＬに対応しているため、リモートアクセス用途などで手軽に導入できる。

イのＷＡＦは、外部ネットワークからの不正アクセスを防ぐためのソフトウェア（あるいはハードウェア）である。ファイアウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことである。求める答えはイとなる。

ウのクラスタ構成は、複数のコンピュータを連結し、利用者や他のコンピュータに対して全体で１台のコンピュータであるかのように振舞うシステムまたは仕組みのことである。

エのロードバランシング機能は、並列に運用されている機器間での負荷がなるべく均等になるように処理を分散して割り当てることである。

問45　エ

ＩＳＭＳプロセスに関する問題である。

ＩＳＭＳは企業や組織が自身の情報セキュリティを確保・維持するために、ルール（セキュリティポリシー）に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのことである。ＩＳＭＳに求められる範囲は、ISO/IEC15408などが定めるような技術的な情報セキュリティ対策のレベルではなく、組織全体に渡ってセキュリティ管理体制を構築・監査し、リスクマネジメントを実施することである。

ＩＳＭＳの定義としてJIPDECは、「ＩＳＭＳとは、個別の問題ごとの技術対策のほかに、組織のマネジメントとして自らのリスク評価により、必要なセキュリティレベルを定め、プランを持ち、資源配分してシステムを運用することである」、また、「組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがＩＳＭＳの要求する主なコンセプトである」と設定している。

ＰＤＣＡは業務の改善で計画－実施－確認－対応策の４つのフェーズを繰り返すことである。

リスクアセスメントとは、リスクの大きさを評価し、そのリスクが許容できるか否かを決定する全体的なプロセスのことである。具体的には、リスク分析により明確化されたリスク因子に基づき、リスク因子により組織の財務基盤にどのような悪影響を及ぼしうるかを評価し、それにより、どのリスク因子を優先的に対処していくかの優先順位決定し、リスク対処のコストパフォーマンスを上述の財務基盤への影響度も絡めて分析評価し検討する。

アの運用状況の管理はＤの実施、イの改善策の実施はＡの対応策、ウの実施状況のレビューはＣの確認、エの情報資産のリスクアセスメントはＰの計画である。求める答はエとなる。

問46　エ

ＩＳＭＳの確立手順に関する問題である。

ＩＳＭＳは企業や組織が自身の情報セキュリティを確保・維持するために、セキュリティポリシーに基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのことである。組織全体に渡ってセキュリティ管理体制を構築・監査し、リスクマネジメントを実施することである。JIPDECの定義は、「ＩＳＭＳとは、個別の問題ごとの技術対策のほかに、組織のマネジメントとして自らのリスク評価により、必要なセキュリティレベルを定め、プランを持ち、資源配分してシステムを運用することである」、また、「組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがＩＳＭＳの要求する主なコンセプトである」と設定している。

ＩＳＭＳの確立の手順は、リスクの分析と評価、リスク対応のための管理目的および管理策の選択、適用宣言書作成の順序で進める。求める答えはエとなる。

問47　エ

ＰＫＩに関する問題である。

ＰＫＩは公開鍵暗号を使ったセキュリティ技術基盤である。ネットワーク上での盗聴、改ざん、なりすましを防止し、安全な情報通信を可能にするためのデジタル署名技術や製品で構成される。だれでも入手できる公開鍵によって通信データを暗号化し、受信者だけが持つ秘密鍵で復号する。一方で、通信相手が間違いなく本人であることを確認するために、デジタル署名に用いる公開鍵

の正当性を保証する認証局を設けて、電子証明書と公開鍵を発行管理して、通信相手の正当性を証明する。

公開鍵暗号化技術、ＳＳＬを組み込んだWWWサーバ／ブラウザ、Ｓ／ＭＩＭＥを使った暗号化電子メール、電子証明書を発行する認証局構築サーバなど、広範な仕組みや技術を統合することによってＰＫＩは実現できる。

アのディスクアレイはデータを複数のディスクに分散して格納し、並列アクセス処理の向上化と信頼性を実現する。システム障害、媒体障害の復旧には役立つが脅威を除くものではない。

イの仮想化は１台のサーバコンピュータをあたかも複数台のコンピュータであるかのように論理的に分割するサーバ仮想化や、複数のディスクをあたかも１台のディスクであるかのように扱うストレージ仮想化などの技術である。地震や火災の対策にはならない。

ウのＣＲＣは伝送データの誤りの検出が可能であるが、不正アクセスの防止にはならない。

エの公開鍵暗号化方式を用いたデジタル署名は盗聴、改ざん、なりすましを防止し、安全な情報通信を可能にする。求める答えはエとなる。

問48　ア

サーバの二重化の効果に関する問題である。

アの可用性の向上は、ネットワークやコンピュータ内の情報や資源がいつでも利用でき、資格を与えられたユーザが情報システムを適時に使用できる保証を高めることである。

イの完全性は、ネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないことである。

ウの機密性はネットワーク上やコンピュータ内の情報を不適切な人間に見せないことである。

エの責任追跡性は、情報資産が改訂された履歴（ログ）などがたどれる状態を，責任追跡性が保たれているという。

サーバ構成の二重化は、信頼性の向上の手段であり、可用性の向上になる。求める答えはアとなる。

問49　エ

事業継続計画の策定に関する問題である。

ビジネスインパクト分析は不測の事態によって、業務が中断したりシステムが停止したりした場合のビジネスへの影響度を分析することである。

アはＢＣＰの有効性の検証、イは復旧手順の関係者への教育、ウはＢＣＰの内容の見直しであり、エの許容される最大停止時間の決定は不測事態発生時のビジネスへの影響度の分析に関係する内容である。求める答えはエとなる。

問50　エ

ＢＣＰに関する問題である。

ＢＣＰ(事業継続計画)は、企業がビジネスコンティニュイティに取り組むうえで基本となる計画のことである。災害や事故などの予期せぬ出来事の発生により、限られた経営資源で最低限の事業活動を継続、ないし目標復旧時間以内に再開できるようにするために、事前に策定される行動計画である。

アはＢＳＣ、イはＢＰＲ、ウはアウトソーシング、エはＢＣＰとなる。求める答えはエとなる。

問51　エ

ＭＤＭに関する問題である。

アのＢＹＯＤは、企業などで従業員が私物の情報端末などを持ち込んで業務で利用することである。私用で普段から使っているスマートフォンなどから企業の情報システムにアクセスし、必要な情報を閲覧したり入力したりすることである。

イのＥＣＭは、企業や組織における情報の蓄積、管理、運用を統括的、包括的に行うための技術やシステムのことである。

ウのＬＴＥは、第３世代携帯電話のデータ通信を高速化した規格で。第４世代への橋渡しという意味で(第３．９世代)とも呼ばれる。

エのＭＤＭは、企業などで社員に支給するスマートフォンなどの携帯情報端末のシステム設定などを統合的・効率的に管理する手法である。また、それを実現するソフトウェアや情報システムなどのことである。求める答えはエとなる。

問52　エ

ＢＯＹＤに関する問題である。

ＢＯＹＤは､企業などで従業員が私物の情報端末などを持ち込んで業務で利用することである。私用で普段から使っているスマートフォンなどから企業の情報システムにアクセスし、必要な情報を閲覧したり入力したりすることなどを意味する。ＢＹＯＤを導入することで企業側は端末購入費や通信費の一部などのコストを削減することができ、社員側は同種の端末を２台持ちする必要がなくなり、普段から使い慣れた端末で仕事ができるというメリットがある。かかった経費は通信費の一部を会社が補助するといった運用が行われることが多い。

問題点は、端末の設定や導入するソフトウェアの種類などを企業側が完全にコントロールするのは難しい、情報漏洩・ウイルス感染などへの対策や、紛失・盗難時の対応などが複雑になる。業務中に利用できる機能やアクセスできるサイトを制限するといった対応も難しくなるなどがある。通信履歴や保存したデータなどをどこまで会社側が取得・把握するかといったプライバシーとの問題も発生する。

エの従業員が私的に保有する情報端末を業務に利用することであり、セキュリティ設定の不備に起因するウィルス感染などのセキュリティ対策が増大する内容が適切である。求める答えはエとなる。

問53　イ

マルウェア対策に関する問題である。

マルウェアは、コンピュータウイルス、ワーム、スパイウェアなどの悪意のこもったソフトウェアのことである。遠隔地のコンピュータに侵入したり攻撃したりするソフトウェアや、コンピュータウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏洩させたりする有害なソフトウェアである。

マルウェア対策としては、パターンファイルを最新の状態に保つ、最新のソフトウェアを使用する、自動･リアルタイムスキャンをオンに設定しておく、ウイルス対策ソフトは、全社共通の

ものを使用するなどが重要である。

ＯＳやブラウザ、メールソフトなどのソフトウェアは、セキュリティホールを修正したり、セキュリティ上の問題を解決したり、ソフトウェアの不具合を解消したりするための修正プログラムが、インターネット経由で各メーカから提供されいる。これらの修正プログラムを定期的に適用して、ソフトウェアを最新の状態に保つ必要がある。

ウィルスがＰＣの脆弱性を突いて感染しないように、ＯＳやアプリケーションの修正パッチを適切に適用する内容が適切である。求める答えはイとなる。

問54　ア

傍受や盗聴と暗号化に関する問題である。

傍受・盗聴は、通信回線上を転送されているデータを相手に知られないように入手する犯罪の１つである。高度な技術と機器が必要であり、探知は難しい。

アの暗号化は、傍受や盗聴されても直ちに内容が把握されることにならないため、被害を避ける対策としては効果がある。求める答えはアとなる。

イのデジタル署名は、発信者の認証である。

ウのファイアフォールは、システムへの不正アクセスの防止である。

エのメッセージ認証は、通信上での情報の改変やエラーの検査のために有効な手段であり、傍受や盗聴防止には役立たない。

問55　イ

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は送信元は受信先（Ｎさん）の公開鍵を利用して暗号化し、受信先は（Ｎさん）秘密鍵を利用して復号する。求める答えはイである。

問56　ウ

公開鍵暗号方式に関する問題である。

送信者は受信者の公開鍵で暗号化し、受信者は自分の秘密鍵で復号する。求める答えはウとなる。

アの暗号化は送信者の自分の公開鍵が誤りで、受信者の公開鍵である。

イの暗号化は送信者の秘密鍵ではなく、受信者の公開鍵で行い、復号は受信者の秘密鍵になる。

エの暗号化は受信者の秘密鍵ではなく、受信者の公開鍵で行い、復号は自分の秘密鍵で行う。

問57　イ

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は暗号化鍵と復号鍵は等しくなく、暗号化鍵は公開で、復号鍵は秘密であり、求める答はイとなる。

問58　ウ

電子メールの公開鍵暗号化方式による暗号化の問題である。

送信者はＸさん、受信者はＹさんであるから、Ｘさんが使用する鍵はＹさんの公開鍵である。

求める答えはウとなる。

問59　ウ

公開鍵暗号方式に関する問題である。

顧客から注文内容の秘密を商店が守ることであり、商店の関係者以外に秘密にしなければならないため、商店は秘密鍵、顧客は公開鍵を使用する必要がある。求める答えはウとなる。

問60　ウ

暗号方式に関する問題である。

アの公開鍵暗号方式は送信者は受信者の公開鍵を利用して暗号化し、受信者は自分の秘密鍵で復号する。暗号鍵は公開されている。秘密時に配信する必要はない。

イの公開鍵暗号方式は秘密鍵暗号方式と比べて処理方法が複雑なため処理速度も速くはない。単純で高速であるは誤りである。

ウの内容は秘密鍵暗号化方式の鍵管理の方法として実用化されており正しい。求める答えはウとなる。

エの同一の秘密鍵を多数の通信相手に使用すると秘密鍵でなくなるため安全でない。

問61　エ

公開鍵暗号方式に関する問題である。

アは、暗号化鍵、暗号化アルゴリズムは公開であり、復号鍵が秘密である。

イは、暗号化アルゴリズムも公開でよい。

ウは、暗号化鍵は公開で、復号鍵が秘密である。

エの復号鍵は秘密、暗号化鍵は公開は適切である。求める答えはエとなる。

問62　エ

暗号化に関する問題である。

アのＤＥＳは、秘密鍵暗号方式であり、ＲＳＡは公開鍵暗号方式である。

イの公開鍵暗号方式では暗号化鍵を公開する。復号鍵の公開ではない。

ウのデジタル署名に利用するのは公開鍵暗号方式である。秘密鍵方式ではない。

エの秘密鍵暗号方式は暗号化の鍵と復号の鍵は同じである。求める答えはエとなる。

問63　イ

暗号に関する問題である。

アのＤＥＳは秘密鍵暗号方式であり、公開鍵暗号方式ではない。

イのＲＳＡは素因数分解を利用した公開鍵暗号方式である。求める答えはイとなる。

ウの鍵の管理が問題になるのは秘密鍵暗号方式であり、公開鍵暗号方式ではない。

エの公開する鍵は受信者の暗号化鍵であり、復号鍵ではない。

問64　ア

ＤＥＳの暗号化方式に関する問題である。

アのアルゴリズムが公開されている秘密の共通鍵暗号方式である。ＤＥＳの内容であり、求める答えはアである。

イの暗号化鍵を公開し復号鍵を秘密にするのは公開鍵暗号方式であり、ＲＳＡ方式である。

ウの処理に時間がかかり認証機能に優れているのは公開鍵暗号化方式のＲＳＡ方式である。

エの暗号文は必ず解読が可能なものであり、平文に戻すことができないは誤りである。ＤＥＳ方式は鍵の管理が的確に行われると安全性の高い方式である。

問65　ウ

公開鍵暗号方式の暗号化鍵に関する問題である。

アの復号鍵を暗号化鍵から計算によって求めることができるのなら、暗号化鍵が公開されているからもともと暗号化の意味がなくなる。

イの復号鍵を事前に暗号化鍵から計算によって求めることができるなら、暗号化鍵が公開されていることから、暗号化の意味がなくなる。

ウの受信側が暗号化の鍵を知っていることは、受信側しか知らなければ公開鍵で暗号化しても暗号化の意味があることになる。求める答えはウとなる。

エの暗号鍵から算出した復号鍵を受信側に渡しても、暗号鍵が公開されているから、暗号化の意味がなくなる。

問66　ア

共通鍵暗号化方式の名称に関する問題である。

アのＤＥＳは米国の商務省標準局によって制定された共通鍵暗号方式である。求める答えはアとなる。

イのＲＳＡは大きな数の素因数分解の困難性を利用したもので、公開鍵暗号方式である。

ウのエルガマル暗号は離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

エの楕円曲線暗号は楕円曲線上の離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

問67　イ

公開鍵暗号方式に関する問題である。

ア、ウ、エの内容は秘密鍵暗号方式であり、イの内容が公開鍵暗号方式である。求める答えはイとなる。

問68　イ

デジタル署名に関する問題である。

公開かぎ暗号方式で、送信者を保証する方式は、送信者が自分の秘密かぎで暗号化し、受信者が送信者の公開かぎで復号する場合である。求める答えはイとなる。

問69　ウ

暗号文に関する問題である。

ＤＥＥＲ→ＥＲＤＥ　　ＤＩＤＤ→ＩＤＤＤ　　ＲＥＡＭ→ＥＭＲＡ　　ＤＥＥＰ→ＥＰＤＥ

従って、ＥＲＤＥＩＤＤＤＥＭＲＡＥＰＤＥとなり、求める答えはウである。

問70　イ

排他的論理和の論理演算によって暗号化する問題である。

元のデータとかぎの１０１０との排他的論理和が００１０となる元のデータを求めればよいことになる。答は１０００となり、求める答えはイとなる。

問71　ウ

シーザ暗号に関する問題である。

ｃ→ｇ、ａ→ｅ、ｓ→ｗ、ｈ→ｌであるからＮ＝４である。求める答えはウである。

問72　エ

デジタル署名に関する問題である。

デジタル署名は電子メールの送信者が間違いなく本人であることや、文書やデータが改ざんされていないことを確認するための方法である。文書の送信者が文書をハッシングと呼ばれる手法でダイジェストという短いコードに変換し、このダイジェストを送信者の秘密鍵で暗号化したものがデジタル署名となり、これを元の文書とともに受信者に送付する。受信者はデジタル署名を送信者の公開鍵で復号し、ダイジェストを作成する。送信者のダイジェストと受信者が再作成したダイジェストが一致すれば、送信者本人からのメールであることを確認できる仕組みである。

アは受信者の公開鍵と秘密鍵であり、誤りである。

イは受信者の公開鍵が誤りである。

ウは受信者の秘密鍵が誤りである。

エの送信者の秘密鍵と公開鍵が正しい。求める答えはエとなる。

問73　イ

公開鍵暗号方式に関する問題である。

公開鍵暗号方式は通信文を送信する場合、送信元で公開鍵により暗号化し、受信先で専用の秘密鍵で復号する方式である。暗号化する鍵と復号する鍵が異なり、片方の鍵を公開し、もう一方の鍵は秘密にした暗号化方式である。代表的なものにＲＳＡ方式がある。公開鍵から秘密鍵を発見することは不可能であり、公開鍵を管理する必要がない。秘密鍵は自分だけが持てばよいので、鍵管理が簡単で安全度が高い。論理が複雑なため処理時間が長くなり、処理速度は共通鍵方式よりも遅い。公開鍵暗号を守秘に使う場合、送信者は受信者の公開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、元の平文を得ることができる。鍵の配布やデジタル署名に利用される。

アのＡＥＳは共通鍵暗号方式である。

イのＲＳＡは素因数分解の計算の困難さを利用した公開鍵暗号方式である。求める答はイとなる。

ウの公開鍵暗号方式の利用者が増加しても、鍵は公開されているので煩雑にはならない。

エの公開するのは受信者の暗号化鍵である。

問74　エ

公開鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。

イのＤＳＡは、離散対数問題に基づく公開鍵暗号を応用して開発された、デジタル署名方式の一つである。

ウのＩＤＥＡは、ＰＧＰやＳＳＨなどで使用される秘密鍵暗号方式である。

エのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。求める答えはエとなる。

問75　エ

電子署名に関する問題である。

電子署名は送信元は送り手の秘密鍵を用いて署名文(暗号文)にし、受信先は送り手の公開鍵を用いて平文にする。通常、平文を署名文に変換することを復号、署名文を平文に変換することを暗号化という。

ａは送り手の秘密鍵、ｂは送り手の公開鍵であり、求める答えはエである。

問76　エ

ディジタル署名の鍵に関する問題である。

ディジタル署名の作成には発信者の秘密鍵を使用し、ディジタル署名の検証には発信者の公開鍵を使用する。求める答えはエとなる。

問77　エ

デジタル署名に関する問題である。

署名が意味があるのは署名者しか署名できないからである。署名の内容を暗号化する場合に署名者しか暗号化の方法が判らないようにする必要がある。デジタル署名は公開鍵暗号方式を利用して署名者が秘密鍵をもち、署名を受信する人が署名者の公開鍵でメッセージを平文に復号するので、信頼性と公開性の上で意味のあるものになる。

アの受信者が署名鍵で平文に戻しても、多くの人が署名鍵を持つことになると署名の意味がなくなってしまうことになる。

イの送信者が署名の意味を関係者以外に分からないようにすると、関係者以外は署名の内容を把握することができない。関係者のみが知るための手段が問題になる。

ウの平文の冗長性のみで署名が可能になるならば暗号化の意味がない。もともと暗号化は冗長性を加えて意味不明のメッセージに一定のルールによって行う手段であり、他人がそれを実行できないところに価値がある。署名の信頼度を高める技術が問題になる。

エは公開鍵暗号方式の仕組みであり、正しい。求める答えはエとなる。

問78　エ

デジタル署名のメッセージの暗号化の方法に関する問題である。

発信者は自分の秘密鍵でメッセージのハッシュ値を暗号化する方法で行う。求める答えはエと

なる。

アは相手の公開鍵でなく、自分の秘密鍵である。

イは相手の秘密鍵でなく、自分の秘密鍵である。

ウは自分の公開鍵でなく、自分の秘密鍵である。

問79　ウ

ディジタル署名に用いるハッシュ関数の特徴に関する問題である。

ドキュメントや数字などの文字列の羅列から一定長のデータに要約するための関数・手順のことをハッシュ関数という。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。１方向関数による生成であるので、ハッシュ値を変更しないまま元データを改ざんすることはできないため、認証と完全性検査に用いられる。

メッセージダイジェストからメッセージを復元することは困難である。求める答えはウとなる。

問80　ウ

認証に関する問題である。

認証には、相手認証とメッセージ認証がある。

相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。単純な方式ではパスワードを使用する。第三者のなりすましに対する対策である。

メッセージ認証には、データの完全性と否認防止がある。データの完全性は、通信途上で、内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は、送ったことを否定できないことの保証であり、受信側は、受け取ったことを否定できないことの保証である。

相手認証以外の目的であるから、メッセージ認証である。ウの署名が行われた後で、メッセージに変更が加えられていないかどうかを確認することである。求める答えはウとなる。

ア、イは相手認証、ウはメッセージ認証である。

エは盗聴であり、認証では対応できない。

問81　エ

ディジタル署名に関する問題である。

ディジタル署名が使用される認証には、相手認証とメッセージ認証がある。相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。メッセージ認証は、データの完全性と否認防止がある。データの完全性は、通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。

ディジタル署名は、ソフトウェアの作成者を認証するものであり、署名後変更されていないことを証明するものである。従って、インターネットで公開されているソフトウェアの署名はデータの完全性を保証するものである。求める答えはエとなる。

問82　エ

デジタル署名に関する問題である。

デジタル署名は、電子メールの送信者が間違いなく本人であることや、文書やデータが改ざんされていないことを確認するための方法である。

デジタル署名は秘密鍵と公開鍵を組み合わせた個人認証システムである。

送信元の秘密鍵を用いて復号し、受信先で送信元の公開鍵を用いて暗号化し、元の平文としての署名を得る。文書の送信者が文書をハッシングと呼ばれる手法でダイジェストという短いコードに変換し、このダイジェストを送信者の秘密鍵で暗号化したものがデジタル署名となり、これを文書とともに受信者に送付する。受信者はデジタル署名を送信者の公開鍵で復号し、ダイジェストを作成する。送信者のダイジェストと受信者が再作成したダイジェストが一致すれば、送信者本人からのメールであることを確認できる仕組みである。

発信者は自分の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、相手の公開鍵でさらに暗号化することになる。求める答えはエとなる。

問83　ウ

ディジタル署名に関する問題である。

デジタル署名は、個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

アの第三者に情報が漏れるかどうかはディジタル署名では確認できない。

イの発信された注文がＢ商店についてかどうかは確認できない。

ウの発信者がＡさんであることは確認できる。求める答はウとなる。

エのＡ氏に商品を売ることの許可は確認できない。

問84　ウ

公開鍵暗号方式に関する問題である。

ＡからＢに通信文を送信する時に、暗号化に使用する鍵は受信者Ｂの公開鍵である。ＡはＢの公開鍵で暗号化し、ＢはＢの秘密鍵で復号する。求める答えはウとなる。

問85　ウ

ディジタル署名に関する問題である。

ディジタル署名が使用される認証には、相手認証とメッセージ認証がある。相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。メッセージ認証は、データの完全性と否認防止がある。データの完全性は、通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証

である。

ディジタル署名は、ソフトウェアの作成者を認証するものであり、署名後変更されていないことを証明するものである。従って、インターネットで公開されているソフトウェアの署名はデータの完全性を保証するものであり、メッセージが改ざんされていないことを保証する。求める答えはウとなる。

問86　エ

暗号化技術の利用目的に関する問題である。

アの否認防止はメッセージ認証によって実現できる。公開鍵暗号方式の利用である。

イの相手認証は公開鍵暗号方式を利用すれば実現する。

ウの守秘は暗号化によって実現できる。

エの通信途中での喪失は防止することができない。途中で情報が失われても、内容が理解できないとか理解に時間がかかる場合には対策を講じることが可能になる。そのために暗号化は意味のあることになる。求める答えはエとなる

問87　ア

盗聴防止対策に関する問題である。

盗聴は電話回線上の通話や通信ネットワーク上で送受信されているデータを不正に傍受する子である。ログインに必要なＩＤとパスワード、クレジットカード番号、銀行口座番号なとが対象になる。盗聴には電話盗聴、室内盗聴、電子盗聴などがある。盗聴を防止する手段としては暗号化がある。

アの通信の暗号化は盗聴防止に効果がある。求める答えはアとなる。

イのＩＰアドレスの制限、ウのパスワードの設定、エのポート番号の変更などはアクセス制御の役割は果たすが盗聴防止には役立たない。

問88　エ

通信文の共通鍵を用いた暗号化方式の問題である。

通信文は共通鍵方式で暗号化し、共通鍵の送信を受信者の公開鍵を用いて暗号化し、受信者は自分の秘密鍵で共通鍵を得て、その共通鍵を使用して通信文を平文に復号する。

セキュリティ上の効果は電子メールの本文の内容の漏洩の防止である。求める答えはエとなる。

問89　ウ

ディジタル署名に関する問題である。

アのウィルスチェックは、コンピュータウィルスを発見・駆除するための処理である。

イのジャンクメールフィルタは、迷惑メールを仕分けし、取り除くフィルタである。

ウのデジタル署名は、受発注情報の改ざん、なりすまし、否認の防止に役立つ。求める答えはウとなる。

エのファイアフォールは、システムへの不正アクセスの防止である。

問90　エ

Ｓ／ＭＩＭＥに関する問題である。

アのＢＡＳＥ６４は、電子メールに画像などのバイナリデータを添付する際に、中身を文字列データに置換する方式の一つである。

イのＧＺＩＰは、ファイル圧縮形式の一つである。

ウのＰＮＧは、画像フォーマットの一つである。

エのＳ／ＭＩＭＥは、電子メールを暗号化するための方式である。求める答えはエとなる。

問91　イ

Ｓ／ＭＩＭＥに関する問題である。

Ｓ／ＭＩＭＥは電子メールの暗号化と電子署名に関する規格である。インターネット電子メールの標準仕様であるＭＩＭＥを拡張したプロトコルである。なりすまし、盗聴、改ざんといった電子メールに関する不正行為を防ぐための機能を提供している。Ｓ／ＭＩＭＥではＰＫＩを用いるため、認証局で発行する公開鍵証明書を用いて電子署名の正当性を保証している。

Ｓ／ＭＩＭＥの機能は内容の暗号化と署名である。求める答えはイとなる。

問92　ア

ＩＰsecに関する問題である。

ＩＰsecは、暗号技術を用いて、ＩＰパケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである。ＩＰsecはネットワーク層のプロトコルを保護するので、暗号化がサポートされていない上位層やアプリケーションでもセキュリティの確保が可能になる。ＩＰｖ４ではオプションとして使用することができるが、次世代のＩＰｖ６では標準で実装される。

アのＩＰsecは、ネットワーク層でＩＰによる通信を暗号化するためのプロトコルである。求める答えはアとなる。

イのＰＰＰは、２地点間で回線をつなぎリンクを確立するためのプロトコルである。パソコンからプロバイダのルータまでの間を電話回線でつなぐ場合に利用する。

ウのＳＳＨは、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルで、ＰＯＰ３やＦＴＰなどネットワーク上に平文のパスワードが流れてしまう既存のプロトコルを安全に使用する技術として広く利用される。

エのＳＳＬは、Ｗｅｂブラウザと Ｗｅｂサーバ間の通信を暗号化して安全にデータをやり取りするためのプロトコルである。

問93　エ

コンピュータ不正アクセス対策基準に関する問題である。

コンピュータ不正アクセス対策基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。システムユーザ基準、システム管理者基準、ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準から構成される。

この基準で考えられている「不正アクセス」とは、システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うことである。

「システムユーザ」が実施すべき対策として、パスワード及びユーザＩＤ管理、情報管理、コンピュータ管理、事後対応、教育及び情報収集、監査ついてまとめられている。

アの監視効率向上のため単純にネットワーク相互接続したり、ファイルを共有することは、セキュリティ上問題がある。

イの利用者ユーザＩＤの共有は問題がある。ユーザＩＤは個人単位に設定するのが原則である。

ウのシステム管理者が全ての権限をもつ利用者ＩＤを常に使用するのは不適合である。システム管理者が不正を働く危険性がある。

エのセキュリティ方針の文書化、定期的な研修は適合している。

問94　エ

利用資格の正当性チェックと利用状況の把握に関する問題である。

ユーザＩＤはユーザの識別子で、そのユーザがそのシステムを使う権利があるかどうかを判断するのに利用する。ユーザＩＤとパスワードの差異の認識が重要である。

アのＩＰアドレスはＴＣＰ／ＩＰで通信する場合に通信元や通信先を識別するためのアドレスである。

イのアクセス権はデータやプログラムを読み書きし､それを利用することを認めた権利である。

ウのパスワードは正当なユーザかどうかを確認するための合い言葉である。

エのユーザＩＤはコンピュータの利用時にユーザを認識するために、個々のユーザに与えられた番号であり、英字と数字が用いられる。システムへのアクセス権を判断するのに利用したり、使用実績の把握に用いる。求める答えはエとなる。

問95　ア

インターネットのセキュリティに関する問題である。

アのデータベースサーバを利用する場合に不正アクセスの防止やデータの改ざん対策が必要になる。求める答えはアとなる。

イの暗号化は、第三者へ内容が漏洩しないようにするために、ある一定の規則に従ってデータを変換することである。暗号化は電子メールの到達確認とは異なる。

ウの利用者認証システムは、ネットワーク経由でコンピュータにアクセスしてくるユーザーが登録済みか否かを信頼できる方法で確認するソフトウエアである。中心部分は認証サーバと呼ぶソフトウエアで、ユーザーの名前やパスワードなどを一括管理する。インターネットを利用するためには必ずしも必要としない。個人ユーザがプロバイダーと契約してインターネットを利用する場合には、プロバイダーのシステムを経由するために認証が必要になるだけである。

エのファイアウォールは、インターネットとＬＡＮとの間に置くことでデータ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを守る仕組みである。ファイアウォールを設置しても社内からの重要情報の流出を自動的に防止できない。

問96　エ

セキュリティ技術に関する問題である。

アのフォルトトレラント技術は、システムの一部に障害が起きても全体を停止させずに稼働を続け、その間に復旧を図る考え方である。この技術は地震や火災に対しては意味がない。

イの盗聴は、電話回線上の通話や通信ネットワーク上で送受信されているデータを不正に傍受することであり、ファイアフォールやディスクアレイシステムで防ぐことはできない。

ウのＣＲＣ方式は、バーストエラーやランダムエラーなどの通信上の誤りを検出する方式であり、データの不正アクセス防止の対策にはならない。

エのメッセージの改ざんやなりすまし防止にディジタル署名は効果的である。求める答えはエとなる。

問97　イ

ユーザ認証の問題である。

パスワードは正当なユーザを確認するための合い言葉であり、設定上次のことに留意する。

① パスワード入力の際にパスワード自体の表示や印字を抑止する。
② パスワードの有効期限を設定する。
③ パスワードを暗号化してファイル上に格納する。
④ パスワードを保存するパスワードファイルのアクセスを制限する。
⑤ 高度パスワードを適用し、類推できるようなパスワードの使用を制限する。
⑥ 初期パスワードの設定をする。
⑦ 初期パスワードは、初回だけ仮パスワードで情報処理システムへアクセスを許し、ファイルアクセス前にユーザ側で正式のパスワードに変更しなければならない方法にする。

アのパスワードの変更は、有効期限を設定し、絶えず変更する必要がある。変更を禁止するのは誤りである。

イのコールバックは本人であるかどうかの認証方法の一つて、折り返し電話をすることで本人確認をする方法である。求める答えはイとなる。

ウのユーザがパスワードを確認できるように端末に表示するのは誤りで、パスワードの表示や印字は行ってはならない。

エの一定回数間違ったからといって、親切に相手に通知するのは誤りである。

問98　エ

データの改ざんや破壊防止に関する問題である。

災害や情報セキュリティのシステム的対策として次のことが考えられる。

① システム・回線の多重化等のフォルトトレラント技術、
② バックアップ技術、無停電電源などの信頼性技術、
③ 暗号、ユーザ認定、アクセス制御などの情報セキュリティ技術

データの改ざんや破壊を防止する最も効果的な方法はセキュリティ技術であり、ファイルへのアクセス権限の設定が効果的である。

ア、ウの内容は障害発生時の回復処理には必要であるが、改ざんや破壊防止には役立たない。

イは改ざんの検出には役立つが防止にはならない。

エのファイルへのアクセス権限の設定はデータの改ざんや破壊防止に効果的である。求める答えはエとなる。

問99　ウ

ユーザＩＤ管理に関する問題である。

あるコンピュータをユーザーが使う時に、コンピュータはユーザーＩＤを使って、そのユーザーがそのコンピュータを使う権利があるかどうかを識別する。ＩＤは各ユーザーの識別子であり、このＩＤを管理することをユーザＩＤ管理という。

ユーザ管理の主な目的は次の通りである。

①　資源利用の把握に活用し、合わせて発生する費用の配賦に使用する。

②　資源の将来的な設備増強など設備計画に活用する。

③　障害発生時に影響の及ぶユーザへ迅速な連絡に活用する。

④　利用権を持たない利用者を制限し、情報処理システムの安全性や、信頼性、性能維持の確保に利用する。

⑤　ユーザ支援の一貫として､情報処理システム広報作業など効率性向上のために利用する。

ユーザＩＤの付け方は次の通りである。

①　英数字の組合せで構成されたものが一般的である。

②　個人単位のユーザに付与する。ユーザがどのような利用者であるかも体系づける。

③　先頭に利用者の作業内容を示す英字を付ける。

④　ユーザＩＤによるアクセス権を設定する。

アのプロジェクトで皆同じユーザＩＤを用いるのは間違いで、個人単位に付与する。個人の識別子を用いて、ユーザの資源利用の実態把握と不当アクセス防止などの管理を行う。

イの同一人が複数のＩＤカードをもつのは管理上不合理になる。アクセス権の設定などのユーザＩＤに付与する権限か不明確になる。

ウのユーザＩＤの権限を設定する場合に権限は必要最小限のものにし、利用目的、利用期限を明確にする。求める答えはウとなる。

エのユーザＩＤの抹消は利用目的が完了した時点で直ちに抹消する必要がある。

問100　エ

パスワードの文字数と種類の数、その調査に必要な時間を求める問題である。

パスワードの文字数は５文字で、使用できる文字は英字２６文字、数字１０文字の計３６文字である。これらの文字でできるパターンの種別は36^5＝６０４６６１７６となる。

一つのパスーワードの調査に０．５秒必要であるから、全部のパスワードの検査には次の時間がかかることになる。

３０２３３０８８(秒)→８３９７(時間)→３５０(日)→１(年)

求める答えはエとなる。

問101　ア

データベースの不正利用防止の方法に関する問題である。

アのアクセス権の設定は正当な利用者のみにアクセスを許可するものであるから、不正な利用者のアクセスを防止することができる。求める答えはアとなる。

イの一貫性維持の制御は状態の変化が正しく反映されるとか矛盾を発生させない性質であり、複数のデータベースで論理矛盾を発生させないように、矛盾が発生する恐れがある場合には、す

べてのデータベースを元の状態に戻すことによって回避する方法である。不正利用者のアクセス防止にはならない。

ウのデータのカプセル化は、データとその操作法を一体にすることによって独立性を保つことは可能になるが不正アクセスの防止にはならない。

エのファイルの二重化は故障時の停止を防止でき信頼性の向上にはなるが、不正利用者のアクセス防止にはならない。

問102　エ

ＩＣカードの暗証番号に関する問題である。

利用者認証を行うには、ＩＣカードのユーザＩＤとそのカードを使用しているのが本人であることを確認する暗証番号が必要である。

ＰＩＮコードは、クレジットカードやキャッシュカードの利用に際し持ち主の本人確認のために使われる、秘密の識別番号である。カードを提示した人物が所有者本人であることを確認するために照合される番号で、他人に知られると成りすまして悪用される恐れがあるため、秘密にして暗誦しなければならない。銀行のキャッシュカードなど、多くの場合に４桁の番号が使われる。

アの共通な暗証番号の設定では本人確認は不可能である。

イのＩＣカードの表面に印字している数字情報を組み合わせて暗証番号を作成すると、第三者が推測可能な番号となり、本人確認の機能にはならない。

ウの失効処理の順序が逆である。

エのＩＣカードを配送する場合には暗証番号は同封しない。暗証番号の配送が必要な場合は別経路で配送する。求める答えはエとなる。

問103　ア

パスワードに使用する文字の種類を問題にしている。

パスワードに使用する文字の種類をＭ、パスワードの桁数をｎとするとき、設定できるパスワードの個数は、場合の数の計算で求めると、各桁にＭ通りの文字が使用できるため、M^nとなる。求める答えはアである。

問104　エ

ＩＣカードの暗証番号に関する問題である。

利用者認証を行うには、ＩＣカードのユーザＩＤとそのカードを使用しているのが本人であることを確認する暗証番号が必要である。

ＰＩＮコードは、クレジットカードやキャッシュカードの利用に際し持ち主の本人確認のために使われる、秘密の識別番号である。カードを提示した人物が所有者本人であることを確認するために照合される番号で、他人に知られると成りすまして悪用される恐れがあるため、秘密にして暗誦しなければならない。銀行のキャッシュカードなど、多くの場合に４桁の番号が使われる。

アの共通な暗証番号の設定では本人確認は不可能である。

イのＩＣカードの表面に印字している数字情報を組み合わせて暗証番号を作成すると、第三者が推測可能な番号となり、本人確認の機能にはならない。

ウの失効処理の順序が逆である。

エのＩＣカードを配送する場合には暗証番号は同封しない。暗証番号の配送が必要な場合は別経路で配送する。求める答えはエとなる。

問105　イ

パスワード運用方法に関する問題である。

パスワードは利用者の認証を行うために利用する数字や文字列である。利用制限をかけているコンピュータや共有資源では、ユーザＩＤとパスワードによって利用者であることを認証する。

パスワードは次の特徴をもっている。

①　正当な利用者以外に漏らしてはならない

②　推測しやすいパスワードを設定すると、悪意ある第三者による不正利用の恐れがある。

③　パスワードは数字や文字・記号を混在させた推測しづらいものを使用する。

④　パスワードは有効期限を設定し、適宜変更する。

⑤　パスワードは暗号化してファイルに格納する。

アの内容は、パスワードは本来、本人のみが認識でき変更できるものでなければならないため、管理者と言えども他人のユーザＩＤとパスワードの一覧表を作成し、いつでも確認できるようにすることは誤りである。

イの利用者がいつでも変更できるようにすることはパスワードの運用管理方法として適切である。求める答えはイとなる。

ウの現在利用されていないユーザＩＤとパスワードの再利用は、不正アクセスや情報処理システムの破壊などのトラブルの原因になる。従って、使用停止処理を必ず行う必要がある。

エの利用者登録申請書が到着する前に、ユーザＩＤや仮のパスワードを登録することは間違いである。

問106　エ

ＣＡに関する問題である。

ＣＡはインターネットのメールやWWWページなどにデジタル署名するときに付与する電子印鑑証明書を発行するシステムである。求める答えはエである。

問107　ウ

パスワードを用いた利用者認証に関する問題である。

利用者認証は、相手が本当の相手であることを確認する手段であり、単純な方式では、利用者ＩＤとパスワードを組み合わせて利用する。その際、パスワードの盗難防止の目的で、パスワードをハッシュ値に変化して使用する。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して登録し、認証時に入力されたパスワードをハッシュ関数で変換して比較しても利用者認証にはならない。

イの利用者ＩＤをハッシュ関数で変換して登録し、認証時に入力された利用者ＩＤをハッシュ関数で変換しても、本人の確認は不十分である。

ウのパスワードをハッシュ関数で変換して登録し、認証時に入力されたパスワードをハッシュ関数で変換し、比較すると本人の確認は可能である。求める答えはウとなる。

エのパスワードをハッシュ関数で変換して登録し、認証時に入力された利用者ＩＤをハッシュ関数で変換しても、本人の確認は不十分である。

問108　ウ

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

認証局の主な役割には次のものがある。

① 申請者の公開鍵にディジタル署名を付したディジタル証明書を発行する
② ＣＲＬ(証明書失効リスト)を発行する
③ ＣＰＳ(認証局運用規定)を公開する
④ ディジタル証明書を検証するための認証局の公開鍵を公開する
⑤ 認証局の秘密鍵を厳重に管理する

失効した(効力をなくした)ディジタル証明書の一覧を発行する内容が適切である。求める答えはウとなる。

問109　エ

パスワードの盗難防止に関する問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して、登録パスワードをそのまま保管していると、盗難時には、パスワードがそのまま使用されることになる。

イのパスワードファイルを圧縮して保管していても、復元すればパスワードを知ることができるため無意味である。

ウのパスワードをそのまま登録していると、ファイルの盗難時にパスワードの内容がそのまま相手に知られてしまう。

エのパスワードをハッシュ関数を使用して、ハッシュ値を求めていると、ファイルを盗まれても直ちに内容が相手に分かることがない。

問110　ア

メッセージ認証に関する問題である。

認証には相手認証とメッセージ認証がある。相手認証はある人が他の人に自分が確かに本人であると納得させる事をいう。本人固有の情報(名前、所属、住所、電話番号)を伝えたり、指紋、虹彩等のバイオメトリクス情報を伝えたり、パスワードを入力したり、合言葉を認証者に言ったり、ＩＣカードを認証機械に通すことによって行われる。メッセージ認証はメッセージの同一性の保証であり、コンピュータウイルス、不正侵入等を使った破壊行為によりメッセージが変更されていない事を保証する為の手続きである。メッセージmに対しそのハッシュ値Ｘ＝Ｈ(m)を計算し、Ｘを安全なな場所に保管する。mが改竄されて別のメッセージMになっていた場合、Ｘ≠Ｈ(M)なのでメッセージが改竄された事が分かる。

アの改ざんの有無を検出するはメッセージ認証である。メール本文をハッシュ値と比較するのはメッセージ認証の方法である。求める答えはアとなる。

イの盗聴は電話回線上の通話や通信ネットワーク上で送受信されているデータを不正に傍受することである。

ウのなりすましは他者のユーザＩＤやパスワード、ＩＰアドレスなどを使用して、他者であるふりをしてシステムに進入して不正行為を行うことである。

エのメールの送達確認はメールが目的の相手に無事送られたかどうかを確認することである。

問111　ア

認証局に関する問題である。

電子商取引(ＥＣ)は、コンピュータとネットワークを利用して企業間の商取引や企業と消費者の直接取引を行う。ＥＣを実現するために各企業はインターネットを活用したプライベートのポータルサイトを構築したり、業界共通のパブリックなポータルサイトに接続するなどして、顧客からのアクセス機会を増やすことを行う。

電子認証システムは、デジタル署名技術と認証局、電子証明書を用いることにより、取引者間の相互認証を実現する仕組みである。電子証明書は、インターネットを利用する電子決済などのために、利用者の正当性を保証する証明書で、この証明書は第３者の認証機関が発行する。電子証明書の技術は、公開鍵暗号方式を利用し、公開鍵のデータが正当であることを証明するために、認証機関はこのデータにデジタル署名をする。デジタル署名を使用するシステムでは、各ユーザとそのユーザの公開鍵との対比関係が第三者機関によって保証されていなければならない。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認後に正しいユーザであることを保証する所有者の識別情報や公開鍵などを記載した電子証明書を発行する。

認証局が発行するのは、取引当事者の公開かぎに対する電子証明書である。求める答えはアとなる。

問112　エ

Ｘ、Ｙの２者間での認証に関する通信の問題である。

ＹがチャレンジコードをＸに送信し、ＸはレスポンスコードをＹに返信し、Ｙが確認する仕組みであるから、ＹがＸを認証することになる。求める答えはエとなる。

問113　エ

電子商取引における認証の役割に関する問題である。

電子認証システムは、デジタル署名技術と認証局（ＣＡ）、電子証明書を用いることにより、取引者間の相互認証を実現する仕組みである。

電子証明書は、インターネットを利用する電子決済などのために、利用者の正当性を保証する証明書で、この証明書は第３者の認証機関が発行する。電子証明書の技術としては公開鍵暗号方式を利用するのが一般的である。公開鍵のデータが正当であることを証明するために、認証機関はこのデータにデジタル署名をする。

商取引における取引相手の確認やデータ改ざんの有無の確認は、メッセージ認証やデジタル署名の技術を利用することによって実現できる。署名の検証者は署名者の正しい公開鍵を用いることによって可能となる。デジタル署名を使用するシステムでは、各ユーザとそのユーザの公開鍵との対比関係が第三者機関によって保証されていなければならない。

エの第三者機関によって、取引相手の正当性の証明が電子証明書で、求める答えはエとなる。

問114　ア

ハッシュ関数を使用した認証システムの問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止、メッセージ送信者の確認などを図る。

メッセージが送信者Ａからのものであることを確認するとなり、求める答えはアとなる。

問115　ア

メッセージダイジェストに関する問題である。

メッセージダイジェストは、元のメッセージから任意の長さのメッセージを演算処理して特徴的なパターンを生成し、データ通信のメッセージが正しいことを証明する技術である。インターネットの標準技術であるＭＤ５（Message Digest Algorithm 5）では、一方向ハッシュ関数を使った演算により、元のデータの長さに関係なく128ビットのデータを生成する。

メッセージ認証は、受信したメッセージが途中で改ざんされていないかを確認することである。ハッシュ関数の一種であるメッセージダイジェスト関数を用いて求めるメッセージダイジェストを比較して改ざんの有無を確認する。送信メッセージのメッセージダイジェストと受信メッセージのメッセージダイジェストが異なる場合、伝送途中で改ざんがあったと判断する。

メッセージダイジェストは電子署名の基礎技術であり、電子署名ではダイジェストデータをさらに暗号化する。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。求める答えはアとなる。

問116　イ

ＳＳＬに関する問題である。

ＳＳＬは、インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われているWWWやＦＴＰなどのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。

ＦＱＤＮは、インターネットやイントラネットなどのＴＣＰ／ＩＰネットワーク上で、ドメイン名・サブドメイン名・ホスト名を省略せずにすべて指定した記述形式のことである。

アのＳＳＬはＷｅｂだけで使用されるプロトコルではない。

イは適切な記述である。求める答えはイとなる。

ウのディジタル証明書は、各ユーザからの電子証明書の発行依頼を受け、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。ＰＣ単位ではない。

エのディジタル証明書は、共通鍵ではなく公開鍵暗号方式を使用する。

問117　ウ

商取引に関係する認証の問題である。

アのＩＰパケットフィルタリングは、ルーター、ゲートウエイ、ファイア・ウオールなどで、パケットのあて先アドレス、あるいは送信元アドレスとあて先アドレスの組み合わせを調べて、通過させて良いパケットと阻止すべきパケットを区別すること及びその機能である。パケット・フィルタリングは、余分なトラフィックが生じることの抑制と、セキュリティ機能を実現するための方法である。

イのＩＰポート番号はパソコンと周辺機器を接続するインターフェースのコネクタ部分の番号で、ポート番号を通してＩＰパケットは入出力される。ファイアウォールなどで利用される。

ウのＳＳＬは、WWWのブラウザやサーバ間でサーバの認証に利用されたり、通信データを暗号化したりする技術である。求める答えはウである。

エのクッキーヘッダは、WWWサーバーがユーザーを識別・管理するための仕組みである。

問118　イ

ＳＳＬ／ＴＬＳに関する問題である。

ＳＳＬ／ＴＬＳはウェブブラウザとサーバ間の通信を暗号化して安全にデータをやり取りするプロトコルである。

クライアントサーバ間の通信を暗号化するが正しい答である。求める答はイとなる。

問119　エ

RADIUSに関する問題である。

RADIUSは、ネットワーク資源の利用の可否の認証と利用の事実の記録を、ネットワーク上のサーバコンピュータに一元化することを目的とした、ＩＰ上のプロトコルである。常時接続方式のインターネット接続サービス、無線ＬＡＮ、ＶＬＡＮ、コンテンツ提供サービスなどのサービス提供者側設備において、認証とアカウンティングを実現するプロトコルとして幅広く利用されている。

アのＤＥＳは、米国の商務省が標準暗号化方式として制定した共通鍵暗号方式である。

イのＤＮＳは、インターネットに接続されたコンピュータのドメイン名とＩＰアドレスの対応付けや、両者を置き換える機能などを提供する仕組みである。

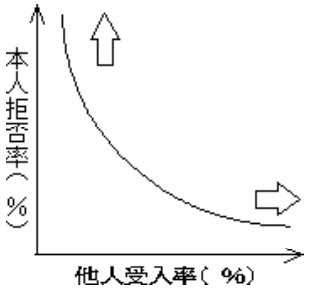
ウのＩＤＳは、ネットワークやコンピュータに対する不正行為を検出し、知らせるためのシステムである。

エのRADIUSは、無線ＬＡＮやＶＰＮ等で利用され、利用者を認証するシステムである。求める答えはエとなる。

問120　ウ

バイオメトリック認証に関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。



アのＦＲＲとＦＡＲは相関関係にある。

イのＦＲＲを減少するとＦＡＲが増大する。

ウのＦＲＲを減少するとＦＡＲが増大する内容は適切である。求める答えはウとなる。

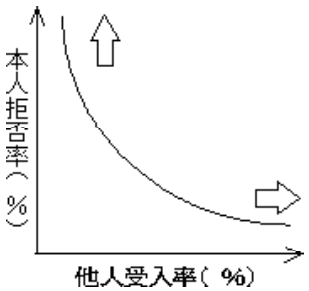
エのＦＲＲを増大するとＦＡＲは減少する。

問121　エ

生体認証システムに関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。

ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。



生体認証システムを導入する場合、本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する必要がある。求める答えはエとなる。

問122　イ

バイオメトリクス認証の問題である。

身体的特徴を利用しているのは、アの血管の分岐点の分岐角度や分岐点間の長さの特徴を用いるもの、ウの瞳孔から外側に向かって発生するカオス状のしわの特徴を用いるもの、エの隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証するものがある。

行動的特徴を用いるものには、署名するときの速度や筆圧から特徴を抽出して認証するものがある。求める答えはイとなる。

問123　エ

ＨＴＴＰＳに関する問題である。

ＨＴＴＰＳは、ＳＳＬ／ＴＬＳプロトコルを用いて、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。ＷｅｂブラウザとＷｅｂサーバの間の通信を暗号化して、盗聴や改竄を防ぐ。

アのサーバ上のファイルの改ざんの検知ではない。

イのウィルス検査の役割はない。

ウのクライアントへの侵入検知はしない。

エの電子証明書を用いてサーバ認証に使用する。求める答えはエとなる。

問124　イ

電子透かしに関する問題である。

アのタイムスタンプは、ファイルなどの電子データにおいて、その作成や更新などが行われた日時を示す情報である。

イの電子透かしは、音声や画像などの電子化されたコンテンツに対して、品質を落とさず利用者に分からない方法で著作権情報を記録する仕組みである。求める答えはイとなる。

ウの電子保存は、情報を電子媒体に保存することである。

エの配達証明は、一般書留とした郵便物や荷物を配達した事実を証明するサービスである。

問125　ウ

ＨＴＴＰＳに関する問題である。

ＨＴＴＰＳは、ＳＳＬ／ＴＬＳプロトコルを用いて、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。ＷｅｂブラウザとＷｅｂサーバの間の通信を暗号化して、盗聴や改竄を防ぐ。

アのＳＱＬインジェクションは、ＳＱＬ文を利用して、ＤＢの改ざんや不正に情報を入手することである。

イのＴＣＰポート８０は、ＨＴＴＰを利用してアプリケーションにデータを渡す場合に利用するポートで、ＨＴＴＰＳはそれ以外のデータ通信を遮断することではない。

ウのサーバとブラウザ間の通信の暗号化は適切な内容である。求める答えはウとなる。

エのパケットフィルタリングは、ネットワーク層型ファイアウォールの機能である。

問126　エ

ユーザ認証に関する問題である。

アの受信データの改ざんの調査を行っても、ユーザ認証にはならない。

イの送信データの暗号化はデータの守秘は守れるが、ユーザ認証にはならない。

ウのデータを発信するコンピュータを特定しても、ユーザを特定することはできない。ユーザ認証にはならない。

エのパスワードはユーザ特有のものであり、ユーザ認証になる。求める答えはエとなる。

問127　イ

コンテンツの改ざんに関する問題である。

何らかの理由でファイルが破損していないか、オリジナルから変更されていないかをチェックする場合には、ファイルの「ハッシュ値」を比較する方法が広く使われている。フリーソフトウェアやシェアウェアでは、配布サイト上にＭＤ５やＳＨＡ１方式によるハッシュ値を掲載し、ダウンロード中にファイルが破損するなどの理由でオリジナルと違ってしまっていないかを確認できるようにしているサイトも多い。求める答えはイとなる。

問128　エ

ファイアウォールに関する問題である。

パケットフィルタリングは、送信元ＩＰアドレス／宛先ＩＰアドレス、送信元ポート番号／宛先ポート番号、接続を開始する方向性、プロトコルに基づき、転送パケットを通過させるかさせないかのアクセス制御を実現することである。パケットフィルタリングによって、あらかじめ設定されていない不正なパケットの流出入を防止する。ルータなどの経路情報を有する装置を利用する。

特定のＴＣＰポート番号をもったパケットだけに、インターネットから内部ネットワークへの通過を許可する。求める答えはエとなる。

問129　イ

アクセス権設定に関する問題である。

３ビットで読取り、更新、作成のアクセス権を設定する。

①　０００はすべてのアクセス権を許可しない。

②　０１１は読取り、更新ができ、作成ができない。

③　１１１はすべてのアクセスが可能になる。

④　以上の内容からアクセス権の設定は、作成・読取り・更新、または作成・更新・読取りになる。

アは、０１０となり、作成はできない。

イは、１００となり、作成だけができる。求める答えはイとなる。

ウは、１０１となり、作成と更新、または作成と読取りになる。

エは、１１０となり、作成と更新、または作成と読取りになる。

問130　ウ

権限の範囲に関する問題である。

アプリケーションは、利用者が必要としている情報をデータベースから検索して、その結果を表示する処理であるから、権限のうち登録や変更、削除などは必要でない。アプリケーションに必要な権限は参照権限であり、更新権限、管理者権限は必要がない。求める答えはウとなる。

問131　ウ

ＤＭＺを使用したサーバ設置法に関する問題である。

ＤＭＺは、インタネットなどの外部ネットワークと社内ネットワークの中間につくられるネットワーク上のセグメントで、外部ネットワークからも内部ネットワークからもファイアウォールなどによって隔離されている。社内ネットワークをインターネットに接続する際に、Ｗｅｂサーバやメールサーバなどインターネットに公開しなければならないサーバは、ＤＭＺセグメントに設置しセキュリティ強化を図ることができる。外部に公開するＷｅｂサーバは、常にリスクに晒されているため、Ｗｅｂサーバーを社内ネットワークに置くとリモートハッキングやマルウェアなどを組み込まれたりした場合、社内ネットワークに接続されているその他のサーバやパソコンがすべて被害を受ける可能性がある。ＤＭＺ内に公開用のＷｅｂサーバを設置して、社内ネットワークと隔離することで、不正侵入された後のマルウェアの感染拡大を防ぐことができ、業務システムなどへの侵入による機密情報の漏洩を防止することが可能になる。

ＤＭＺの構成は、２台のファイアウォールを設置して、インターネット／ファイアウォール／ＤＭＺ／ファイアウォール／社内ネットワークとする方法がセキュリティ強度を高くすることになるが、ファイアウォール1台だけで構成する方法も可能で、１台のファイアウォールが外部セグメントとＤＭＺの間、およびＤＭＺと内部セグメントとの間を特定の通信プロトコルで通信許可の処理を行い対応する。

ＷｅｂサーバはＤＭＺに、データベースサーバは内部セグメントに設置する。求める答えはウとなる。

問132　ア

パケットフィルタリング型ファイアウォールに関する問題である。

ファイアウォールのルールは次のように適用される。

①　番号１で、送信元アドレスをチェックし、一致すれば通過禁止にする。

②　番号２で、宛先アドレス、プロトコル、宛先ポート番号をチェックし、一致すれば通過許可する。

③　番号３で、宛先アドレス、プロトコル、宛先ポート番号をチェックし、一致すれば通過許可する。

④　番号１～３で、ルールが適用されなかったものは、通過禁止にする。

パケットＡは、ルール番号１の送信元アドレスで一致するため、番号１によって通過を禁止する。求める答えはアとなる。

問133　イ

ＨＴＴＰプロトコルに関する問題である。

アのＦＴＰは、ファイル転送プロトコルである。ファイルを転送する場合、ユーザアカウントとパスワードを用いてユーザ認証を行い、認証後に転送を利用できる。

イのＨＴＴＰは、ＨＴＭＬで記述されたファイルを転送するプロトコルである。WWWクライアントとWWWサーバ間で、クライアントからのコンテンツ転送要求に応じて、サーバに格納されているＨＴＭＬファイル、画像、音声、動画像などのコンテンツを転送し、表示する。Ｗｅｂページの閲覧が目的であるからインターネットからの通過を禁止できない。

ウのＳＭＴＰは、インターネット上で電子メールを送信または転送するためのプロトコルである。ＴＣＰのポート番号２５を利用して行う。ユーザの確認、メールボックスの有無、容量の不足などをチェックしながら通信が行われる。

エのＳＮＭＰは、ＴＣＰ／ＩＰのネットワーク管理プロトコルで、ルータやハブなどのネットワーク機器のネットワーク管理情報を管理システムに送る場合の標準プロトコルである。ネットワーク情報の収集に必要なパケットのみを通過させる。

問134　エ

アクセス管理に関する問題である。

アクセス管理はファイルやネットワークなどへのアクセスに関して、ユーザごとにアクセス権を与え、アクセス状況を管理することである。アクセス権は、ユーザがコンピュータのファイルやネットワークなどの共有資源を利用するための権利のことであり、アクセスの禁止や読み取りの許可、書換・削除の許可など、ユーザごとに権利の設定を行う。

ユーザ管理は情報システムの利用者をユーザＩＤなどの識別子を用いて、ユーザの資源利用の実態把握やユーザの不当アクセス防止などの管理を行うことである。ユーザ管理を利用して、ユーザごとにファイルなどの共有資源へのアクセス権を設定し、管理する。

アの利用者ＩＤは利用者個人に対して発行するものであって、原則として業務グループごとに共通のＩＤを使用しない。

イのアクセス権の設定は人事異動など必要が発生する度に変更し、年初にまとめて発行してはならない。

ウの利用者ＩＤの発行は本人の申請に基づいて、担当の業務に関連して発行するものであり、あらかじめ登録しておくものではない。

エの利用者の職務権限に関係なく、業務システムごとにアクセス権を設定するは適切である。求める答えはエとなる。

問135　ウ

ＷｅｂサーバとのＨＴＴＰ通信に関する問題である。

ＨＴＴＰ通信では、ＴＣＰのポート番号８０を使用して、Ｗｅｂサーバとの通信を行う。ＰＣに侵入したマルウェアは、業務上のＷｅｂ閲覧と同じ条件でサーバへのアクセスを行い、侵入を図る。

アのＤＮＳサーバのポート番号は５３、イのＨＴＴＰＳは４４３、ウのＨＴＴＰは８０、エのドメイン名の名前解決に使用されるのはＵＤＰの５３である。求める答えはウとなる。

問136　エ

Ｗｅｂビーコンに関する問題である。

Ｗｅｂビーコンは、Ｗｅｂページに埋め込まれた情報収集用の極めて小さい画像のことで、利用者のアクセス動向などを収集するために用いられる。大手サイトを中心に利用されている。求める答えはエとなる。

問137　ウ

認証デバイスに関する問題である。

アのＩＥＥＥ８０２.１Ｘ(ＥＡＰ-ＴＬＳ)は、無線ＬＡＮなどで利用される認証プロトコルの１つである。ネットワークのセキュリティを高めるＥＡＰ(Extensible Authentication Protocol)に対応し、サーバ／クライアントの双方で電子証明書を利用する方式のためセキュリティが、より強化される。また、電子証明書の保管にＵＳＢ認証トークン、指紋認証トークンなどを用いることで、さらにセキュリティレベルを強化することができる。

イの確実な通信を行える接触型は主に、より堅牢なセキュリティが求められる決済や認証の分野で使われている。非接触型とは、カード内部にアンテナの役目を果たすコイルが内蔵されており、端末のリーダ／ライタから発生している磁界にカードをかざすと無線通信でデータのやりとりができる。鉄道改札や入退室管理など、より利便性を求められるジャンルで活用されている。

ウの虹彩認証は､眼球の黒目に現れる皺のパターンを識別して本人確認を行う認証方式であり、人体の特徴を利用するバイオメトリクス認証(生体認証)の一つである。カメラで眼の部分を撮影し、コンピュータで虹彩のパターンを抽出して認証する。非接触式であるため衛生的で、心理的抵抗が少ない。顔や声のように年をとっても変化することがなく、指紋のような偽造も難しい。認証率も高く、処理するデータ量も少なくて済むという。求める答えはウとなる。

エの静電容量方式の指紋認証デバイスはＬＥＤ照明の下でも正常に認証でき､活用されている。

問138　ア

プルトフォース攻撃に関する問題である。

プルトフォース攻撃は、パスワードの取得のため、辞書ツールを使いあらゆる文字の組み合わせで総当たりを試み、暗号の解読のためには考えられるすべての暗号鍵をリストアップして暗号文の切れ端を復号できるか試みることである。非常に効率の悪い方法であるが、認証失敗回数制限によりＩＤが凍結されない限り、パスワードが取得されてしまう可能性がある。そのためにも定期的にパスワードを変更されることや、判明しやすい「平易な英単語」を含むものは使用しないことが推奨されているのである。

アの１組の平文と暗号文に総当たりで鍵を割り出す方法は、プルトフォース攻撃である。イは線形解読法、ウはサイドチャネル攻撃、エは差分解読法である。求める答えはアとなる。

問139　イ

標的型攻撃メールに関する問題である。

標的型攻撃メールは、特定の組織内の情報を狙って行われるサイバー攻撃の一種で、その組織の構成員宛てにコンピュータウイルスが添付された電子メールを送ることなどによって開始される。以降も持続的に潜伏して行われる標的型攻撃はＡＰＴ攻撃と呼ばれている。標的型攻撃の対象とされる組織は、政府／公共サービス機関、製造業が多く、価値の高い知的財産を保有している組織が対象になっている。

ソーシャルエンジニアリング手法は、コンピュータやネットワークの管理者や利用者、また、その関係者などから、話術や盗み聞き、盗み見などの社会的な手段によって、パスワードなどの保安上重要な情報を入手することである。

アはスパムメール、イは標的型攻撃メール、ウは架空請求詐欺メール、エはフィッシング詐欺

メールである。求める答えはイとなる。

問140　ウ

ＩＳＭＳ適合性評価制度に関する問題である。

ＩＳＭＳは、情報セキュリティを管理するための仕組みで、この仕組みの基準として用いるのが、 国際規格ISO/IEC 27001／日本工業規格 JIS Q 27001「情報セキュリティマネジメントシステム－要求事項」であり、構築されたＩＳＭＳが、ISO27001/JISQ27001に適合していることを、第三者が評価し、認定する制度がＩＳＭＳ適合性評価制度である。ＩＳＭＳのマネジメントシステムの基盤部分は、品質管理マネジメントシステム（QMS）ISO9001や環境マネジメントシステム（EMS）ISO14001などと調和が図られており、ＩＳＭＳ（ISO/IEC 27001)、ＱＭＳ（ISO9001)、ＥＭＳ（ISO14001）をまとめて“三大マネジメントシステム”などと言われている。

アはＩＴセキュリティ評価及び認証制度(JISEC)、イはプライバシーマーク制度、ウはＩＳＭＳ適合性評価制度、エは暗号モジュール試験及び認証制度（JCMVP)である。求める答えはウとなる。

問141　イ

ＬＡＮアナライザに関する問題である。

ＬＡＮアナライザは、通信回線を流れるパケットを捕獲して中身を表示するソフトウェアやハードウェアの総称である。ネットワークを流れるデータの通信量やその変化を調べたり、障害発生時に原因を調査するのに使われる。ＬＡＮアナライザには専用のハードウェアをネットワークに接続して解析するタイプの製品もあるが、多くの製品はソフトウェアで提供されており、コンピュータのネットワークカードが受信したパケットを解析する。ネットワークカードは、パケットの宛先などを読んで自分に関係がなければこれを破棄するが、プロミスキャスモードと呼ばれる特殊な設定にすることで、自分の属するセグメントを流れるすべてのパケットを受信することができる。ＬＡＮアナライザはこれを解析して、パケットの中身を表示したり各種の統計を取ったりすることができる。通信量を記録して時間帯や曜日による変化を表示したり、パケットの送信元や宛先、プロトコルの種類などによる統計を表示することができる。

ＬＡＮアナライザは通信内容を送信者や受信者に気付かれずに閲覧することができるため、暗号化されていないパスワードやクレジットカード番号など、秘密にしたい通信内容の盗聴に悪用される場合がある。外部からの侵入者がこっそりＬＡＮアナライザを仕掛けて、定期的に結果を報告させていたという事例もある。

ＬＡＮアナライザは、ネットワークを通過するパケットを表示できるので、盗聴などに悪用されないように注意する必要がある。求める答えはイとなる。

問142　ア

ワームの検知方針に関する問題である。

ＳＨＡ-256とは､任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順で、最長で２の64乗ビットまでの原文から、256ビットのハッシュ値を算出することができる。2001年に米国家安全保障局（NSA）が開発し、米国立標準技術研究所（NIST）がハッシュ関数の国家標準の一つとして採用した。SHA-224、SHA-256、SHA-384、SHA-512をまとめて「SHA-2」と通称

することがある。

ワームの検知方式は、検知対象ファイルからＳＨＡ-256を使用してハッシュ値を求めたものとデータベース化されているワーム検体ファイルのハッシュ値を比較する方法である。従って、検出できるワームはワーム検体と同一のワームとなる。求める答えはアとなる。

問143　イ

２要素認証に関する問題である。

２要素認証は、ユーザが知っているもの（ID・パスワード）とユーザが持っているもの（複製できない、もしくは複製しづらい機器）を組み合わせてセキュリティレベルを高める方法である。２つの要素が揃っていないと認証を完了することができないため、たとえＩＤ・パスワードが漏えいしてしまっても、もう1つの要素がない限りはログインすることができない仕組みである。

アの２本の指の指紋は、ユーザがもっているものの組合せであり、不適である。

イの虹彩とパスワードは、ユーザがもっているものと知っているものの組合せであるから、２要素認識となる。求める答えはイとなる。

ウの２種類のパスワードは、ユーザが知っているものの組合せであり、不適である。

エの異なる２つのパスワードは、ユーザが知っているものの組合せであり、不適である。

問144　イ

キーロガーに関する問題である。

キーロガーは、キーボードからの入力を監視して記録するソフトである。もともとデバッグなどに利用するツールだったが、複数の人間が利用するパソコンに仕掛けてパスワードやクレジットカード番号などを収集するなど、悪用されることがある。

イのネットバンキング利用時に、利用者が入力したパスワードを収集する。

アはプロキシサーバを悪用した中間者攻撃、イはイーロガーの悪用例、ウはアドウェアの悪用例、エはブラウザのアドオン悪用例である。求める答えはイとなる。

問145　ウ

ディジタル署名に関する問題である。

デジタル署名は、個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

送信者が署名鍵を使って署名を作成し、それをメッセージに付加することによって、受信者が送信者を確認できるようになる。求める答えはウとなる。

アの署名鍵はメッセージダイジェストを暗号化するのに使用する。

イのメッセージダイジェクトの復号に使われるのは送信者の公開鍵であり、ディジタル署名には改ざん部位を特定する機能はない。

エのディジタル署名はメッセージ本文の暗号化を目的としない。

問146　ア

共通鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。求める答えはアとなる。

イのＰＫＩは、公開鍵基盤で、公開鍵暗号を用いた技術・製品全般を指す。

ウのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。

エのＳＨＡ-２５６は、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順である。

問147　イ

スマートフォーンのディジタル証明書に関する問題である。

デジタル署名は個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。

ディジタル証明書が導入されたスマートフォーンは社内システムへのアクセスが許可されたデハイスであること認証している。求める答えはイとなる。

問148　ア

ポートスキャナの利用目的に関する問題である。

ポートスキャンは攻撃の前段階の調査として行われるもので、当該コンピュータの各ポートへ接続開始を要請するデータを送り、どのような反応を返すかを確かめる。これにより、アクセスを受け付けているポートが何番か、どのようなソフトウェアが使用されているか、ソフトウェアの設定がどのようになっているかなどを外部からある程度知ることができ、攻撃に利用可能な設定の不備やソフトウェアの脆弱性などがないかを調べることができる。

ポートスキャンは攻撃者が攻撃対象に対して行う場合のほかに、コンピュータやネットワークの管理者などが自らが管理・運用するコンピュータにセキュリティ上の問題がないか調べるために実行することもある。従って、ポートスキャナーの利用目的は、使用したいポートが通信可能であること、あるいは、使用していないポートが通信不能であることをなどをネットワークの管理者が確認することであり、自分の管理するシステムに弱点がないかどうか調べるためにポートスキャナを利用する。

アはポートスキャナーによる検査、イは利用者ＩＤの管理状況の確認、ウはアクセスログの解析、エはＷｅｂアプリケーション脆弱性診断サービスである。求める答えはアとなる。

問149　ウ

デジタルフォレンジックスに関する問題である。

デジタルフォレンジックは、犯罪捜査や法的紛争などで、コンピュータなどの電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術のことである。

対象となるのはパソコンやサーバ、ネットワーク機器、携帯電話、情報家電など、デジタルデータを扱う機器全般である。事件の関係先の機器を押収して記憶装置から証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から違法行為の証拠となる活動記録を割り出したり、破壊・消去された記憶装置を復元して証拠となるデータを割り出したりといった技術・活動が該当する。また、コピーや消去、改ざんが容易であるというデジタルデータの性質に対応して、データが捏造されたものかどうかを検証する技術や、記録の段階でデータが改ざんできないよう工夫したり､ハッシュ値やデジタル署名などで同一性を保全する技術なども含まれる。

不正アクセスや機密情報漏洩など、コンピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されたが、社会へのＩＴの普及・浸透に伴って、一般の刑事事件などでも捜査や立証に活用されるようになってきている。

ハッシュ関数は、長い文章やデータを固定長のビット列に圧縮する一方向性の関数で、圧縮された値をハッシュ値と呼ぶ。ハッシュ関数は一方向性のため、ハッシュ値から元のデータを復元することはできない。従って、ハッシュ値にディジタル署名を付して、本人性と文書の真正性の証明に利用したり、証拠の保全・開示に広く利用される。

アのパスワードをハッシュ値に変換する説明は、ハッシュ値の機能の説明であり、ディジタルフォレンジックスにハッシュ値を利用する目的ではない。

イは、ハッシュ関数は一方向性のためハッシュ値から元のデータを復元することはできない。

ウのディジタルフォレンジックスにハッシュ値を利用し、原本と複製の同一性の証明する内容は、ハッシュ値を利用する目的である。求める答えはウとなる。

エのハッシュ値に盗聴の有無を検知する仕組みはない。

問150　エ

バックドアに関する問題である。

バックドアは、クラッカーにより侵入を受けたサーバに設けられた、不正侵入を行なうための裏口である。クラッカーはコンピュータへの侵入に成功すると、次回も侵入できるように、管理者に気づかれないようこっそりと侵入経路を確保する。これがバックドアである。バックドアが設置されていると、管理者が不正侵入に気づいて侵入路をふさいでも、クラッカーは前回侵入時に設置したバックドアから再び不正侵入を行なうことができる。

アのシンクライアントエージェントは、シンクライアントからの要求に応じて、処理を代理して行うサーバ側のコンピュータである。

イのストリクトルーティングは、ＲＦＣ２５４３の規則で動作するプロキシサーバである。

ウのディジタルフォレンジックスは、不正アクセスなどコンピュータに関する犯罪行われたときに、原因究明や法的な証拠性を明らかにするための手段や技術の総称である。

エのバックドアは、クラッカーにより侵入を受けたサーバに設けられた、不正侵入を行なうための裏口である。求める答えはエとなる。

問151　ウ

パケットフィルタリングに関する問題である。

通信を行う場合、通信前にポート番号を決める必要がある。通常、ポート番号はアプリケーションごとに標準で決められた番号があり、０～１０２３の番号が割り当てられている。インターネット上のＷｅｂサーバと通信を行う場合はサーバ側のポート番号は８０を用いる。

この問題では、社内のＰＣからインターネット上のＷｅｂサーバにアクセスする場合であるから、Ｗｅｂサーバでのポート番号は８０、ＰＣのポート番号は１０２４以上を用いる。

ＰＣからの発信は、送信元はＰＣ、あて先はＷｅｂサーバ、送信元ポート番号１０２４以上、あて先ポート番号８０であり、サーバからの応答は、送信元はＷｅｂサーバ、あて先はＰＣ、送信元ポート番号８０、あて先ポート番号１０２４以上となる。求める答えはウとなる。

問152　ウ

機密ファイルの廃棄処理に関する問題である。

データの利用に際しては、効率的な利用方法とセキュリティ保持が重要である。廃棄後のデータは管理されないため、重要情報が漏洩しやすい。不要になったデータの廃棄に当たっては、重要データの漏洩を防止するため、厳重なチェックが不可欠である。データの廃棄に当たっては、適切な方法の選択の他にも管理上、留意すべきことがある。特に、セキュリティ上の必要性とデータ保全の必要性を考慮することが重要である。

ＰＣの磁気ディスク上のデータの消去は、特定のビット列をディスクの全領域に上書き処理することによって読み出し不能にする。求める答えはウとなる。

アのデータの圧縮では、伸張の可能性があり、適切ではない。

イのマスタブートレコードを消去しても、静的に読み出すことが可能である。

エのファイル名を変更しても、ディスクから直接、データを読み出すことは可能である。

データ廃棄の方法として次の表に示す処理方法がある。

廃棄手段	内容、特徴、留意点
消磁、消去	磁気ディスクや磁気テープに保存された磁気データを消してから廃棄する 情報システムにおけるデータ廃棄の主要な方法である。 磁気ディスクの全領域を特定のビット列で複数回上書き処理する。
破壊	磁気媒体以外に保存されたデータの廃棄の際に用いる。 焼却が困難な媒体を使用している場合に有効である。
焼却、溶解	紙の上に記録されたデータを廃棄するのに最も適した方法である。 廃棄量が多くなるため、外部の専門業者に委託することが行われる。 セキュリティ上の問題が発生する恐れがあるため、書類の内容が見えない状態で外部に出す配慮が必要になる。
裁断	機密性の高い書類データを廃棄する際に用いられる方法である。 焼却と溶解の組合せが考えられる。

問153　イ

ＳＥＯポイズニングに関する問題である。

アのＤＮＳキャッシュポイズニングは、あるドメインについて偽の情報を発信し、インターネット上のＤＮＳサーバに伝播させ、一般の利用者がそのドメイン内のサーバに到達できないようにしたり、ドメイン所有者の意図しない別のサーバにアクセスを誘導する手法である。

イのＳＥＯポイズニングは、、Ｗｅｂ検索エンジンの検索結果ページの上位に、マルウェアなどが含まれる悪質なＷｅｂサイトを紛れ込ませる操作のことである。検索結果の上位に悪意のあるサイトを並ぶように細工する。求める答えはイとなる。

ウのクロスサイトスクリプティングは、動的Ｗｅｂページの表示内容生成処理の際、Ｗｅｂページに任意のスクリプトを紛れ込ませ、Ｗｅｂサイトを閲覧したユーザ環境で紛れ込んだスクリプトが実行されてしまう悪意のあるスクリプトを注入する攻撃のことである。

エのソーシャルエンジニアリングは、人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法のことで、重役や上司、重要顧客、システム管理者などと身分を詐称して電話をかけ、パスワードや重要情報を聞きだす行為が一例である。

問154　ア

ＳＱＬインジェクションに関する問題である。

ＳＱＬインジェクションは、Ｗｅｂサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてＳＱＬ文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃である。

Ｗｅｂアプリケーションではデータベースの操作にＳＱＬ言語を利用している。ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。このとき、ＳＱＬ文として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり、本来アクセスできない情報を表示させたりすることができてしまう場合がある。

アはＳＱＬインジェクション、イはＤｏＳ攻撃、ウはバッファオーバフロー攻撃、エはクロスサイトスクリプティング攻撃である。求める答えはアとなる。

問155　イ

パスワードリマインダに関する問題である。

パスワードリマインダはユーザがパスワードを忘れた際の救済措置である。本人しか知らない秘密情報をユーザに登録してもらい、パスワード忘れの際には、その情報をユーザ認証の代用とすることで、パスワードを再発行する仕組みである。パスワードリマインダは、認証の機会が増えることでセキュリティが弱くなるため、できればパスワードリマインダを設けない方がよい。

パスワード再設定/再発行手順

パスワードリマインダの「合言葉」が一致したら、パスワード再設定に次の手順を踏むことが推奨されている。

① パスワードリマインダのＷｅｂページ上で１回限り有効なキーをユーザに発行する。

② １回限り有効な別のキーを含むＵＲＬを、ユーザがあらかじめ登録している電子メールアドレス宛送信する。

③　ユーザにそのＵＲＬのＷｅｂページにアクセスしてもらい、先ほどのキーを入力してもらう。

④　キーが照合できたらパスワードの再設定あるいは再発行を行う。

⑤　一定回数以上照合に失敗したら２つのキーは無効にする。

アの場合、暗号化されていないと盗聴されてパスワードが盗まれる。

イの場合の一時的なパスワード再設定ページへのＵＲＬを送るのが安全な方法であり、キーが照合できたらパスワードの再設定あるいは再発行を行う。求める答えはイとなる。

ウ、エの場合、攻撃者が任意のメールアドレスを指定できてしまうため危険である。

問156　イ

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

取引当事者の公開鍵に対するディジタル証明書を発行する。求める答えはイとなる。

問157　ウ

スパイウェアに関する問題である。

スパイウェアは、パソコンを使うユーザの行動や個人情報などを収集したり、マイクロプロセッサの空き時間を借用して計算を行ったりするアプリケーションソフトである。得られたデータはマーケティング会社など、スパイウェアの作成元に送られる。

アはサニタイジング、イはポートスキャンツール、ウはスパイウェア、エは辞書攻撃を行うパスワードクラックツールである。求める答えはウとなる。

問158　ウ

ＳａａＳに関する問題である。

ＳａａＳは、ソフトウェアを提供者側のコンピュータで稼働させユーザーはそのソフトウェア機能をインターネットなどのネットワーク経由でサービスとして使用しサービス料を支払う形態のビジネスである。

ユーザ側の利点は、使用した期間・量だけのサービス料で済み、サービス提供事業者の構築したシステムの機能を利用するためユーザー側のコンピュータ導入・構築・管理などが不要、短期間での利用開始やユーザー数や処理量の急な増減にも対応しやすい、常に最新のソフトウェア機能を使用できるなどがある。

アの障害対策として、利用者側で重要データのバックアップをとっておく必要がある。

イのセキュリティに関しては､利用サービスや利用者ごとに適切なアクセス権限の付与を行い、パスワード設定ルールなども整備する必要がある。パスワードを忘れた場合に備えて、パスワード初期化方法の措置も必要になる。

ウのセキュリティ対策に関しては、ファイアウォールの設定や不正アクセスの管理、ソフトウェアアップデート、セキュリティパッチの適用などのシステムのセキュリティ管理の必要がなく

なる。求める答えはウとなる。

エの管理担当者は利用サービスの内容を理解した担当者を確保する必要がある。

問159　ア

CAPTCHAに関する問題である。

CAPTCHAは、Ｗｅｂページの入力フォームなどで、ロボットによる自動入力を防止するために人間であることを証明させるテストである。歪んだ文字や数字が埋め込まれた画像を表示して、何が書かれているかを入力させる方式がもっとも有名である。画像によるCAPTCHAは、コンピュータによる文字認識処理では読み取れないほど形を歪められたりノイズがかけられた文字や数字が並んでおり、正しい文字を読み取って入力できれば、人間が入力していると推測できる。CAPTCHAによる認証は、迷惑メール業者が無料メールサービスのアカウントを大量取得するのを防いだり、電子掲示板を巡回して広告を自動投稿するプログラムを拒否したり、オンライン投票で大量投票を行うプログラムをブロックしたりするのに使われる。

アのCAPTCHAは、ゆがめたり一部を隠したり画像から文字を判読させ入力させることで、人間以外による自動入力を排除する技術である。求める答えはアとなる。

イのＱＲコードは、自動で高速読み取りができるように開発された２次元コードである。

ウの短縮ＵＲＬは、Webサイトが使うＵＲＬを短く変換したもので、Webサービスとして運営されている短縮ＵＲＬサービスを使うことで、アルファベット数文字程度にする。

エのトラックバックpingは、あるブログからサーバーに対し、更新をしたこととその内容を伝えるためのメカニズムのことである。

問160　イ

rootkitに関する問題である。

rootkitは、クラッカーが遠隔地のコンピュータに不正に侵入した後に利用するソフトウェアをまとめたパッケージである。セキュリティホールなどを利用して他人のコンピュータに不正侵入を行った攻撃者は、侵入を隠蔽するためのログの改ざんツール、侵入口が塞がれても再び侵入できるようにする裏口（バックドア）ツール、侵入に気付かれないための改ざんされたシステムコマンド群などをインストールする。これらを素早く導入するため、一連のソフトを使いやすいパッケージにまとめたものがrootkitで、いくつかの種類がある。これらのソフトのほかにも、ネットワークを盗聴するスニッファツールや、侵入したコンピュータを踏み台にして他のコンピュータを攻撃するための攻撃ツールなどがパッケージされたものもある。

サーバにバックドアを作り，サーバ内で侵入の痕跡を隠蔽するなどの機能がパッケージ化された不正なプログラムやツールはrootkitである。求める答えはイとなる。

アのＲＦＩＤは、微小な無線チップにより人やモノを識別・管理する仕組みである。

ウのＴＫＩＰは、無線ＬＡＮの暗号化に用いられるＷＰＡで採用された暗号化方式である。

エのweb beaconは、Webページに埋め込まれた情報収集用の極めて小さい画像のことである。

問161　ウ

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局で

は、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

認証局の主な役割には次のものがある。

① 申請者の公開鍵にディジタル署名を付したディジタル証明書を発行する

② ＣＲＬ(証明書失効リスト)を発行する

③ ＣＰＳ(認証局運用規定)を公開する

④ ディジタル証明書を検証するための認証局の公開鍵を公開する

⑤ 認証局の秘密鍵を厳重に管理する

ウの利用者やサーバの公開鍵を証明するディジタル証明書を発行する。求める答えはウとなる。

アはＮＴＰ、イ、エは公開鍵を証明するディジタル証明である。

問162　ア

ＷＡＦに関する問題である。

ＷＡＦは、外部ネットワークからの不正アクセスを防ぐためのソフトウェアあるいはハードウェアであるファイアウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールである。

ＷＡＦの特徴は、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。ＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

アはＷＡＦ、イはＷＰＡ２、ウは総合ログ管理システム、エはＵＴＭである。求める答えはアとなる。

問163　エ

ビヘイビア法に関する問題である。

アンチウイルスソフトなどがウイルスの存在を検知する手法の一つで、実行中のプログラムの振る舞いを監視して、不審な処理が行われていないかを調べる方式である。仮想的な実行環境を用意してプログラムを実行し、異常な行動を起こさないか調べる方式と、実際の環境で実行されているプログラムを監視して異常な行動が観測されたら即座に実行を打ち切る方式がある。ウイルス定義ファイルを用いたパターンマッチング法では検知できない新しいウイルスや、ヒューリスティック法での検知が難しいミューテーション型(ポリモーフィック型)などにも対応することができる。

アはチェックサム法、イはコンペア法、ウはハッシュ値比較法、エはビヘイビア法である。求める答えはエとなる。

問164　イ

ＤＮＳキャッシュポイズニングに関する問題である。

ＤＮＳキャッシュポイズニングは、ＤＮＳがＷｅｂへのアクセスやメールの送受信などの際に、接続相手のＩＰアドレスを調べたりする仕組みに対して、ＤＮＳが偽の応答を返すようにしてしまう攻撃手法である。インターネットの利用者が、この攻撃により偽の応答をするようにされたＤＮＳを介してＷｅｂにアクセスすると、気づかないうちにフィッシングサイトに誘導されてしまう。

ＤＮＳキャッシュサーバは、利用者からの任意のドメイン名の名前解決の問い合わせを受け付け、当該ドメイン名を管理するＤＮＳサーバへの問い合わせを代理で行い、結果を利用者に返答するコンピュータやソフトウェアである。この問題の仕組みではＡ、Ｂ各社の従業員は自社のＤＮＳキャッシュサーバを利用して名前解決を行う。

攻撃者はＡ社のＷｅｂサーバのドメイン名に対応するＩＰアドレスをＢ社のＤＮＳキャッシュサーバに記憶させたので、Ｂ社のＤＮＳキャッシュサーバにアクセスし、Ａ社のＩＰアドレスを得ようとする従業員が偽アドレスに誘導されることになる。Ｂ社のＤＮＳキャッシュサーバにアクセスするのはＢ社の従業員である。従って、Ａ社Ｗｅｂサーバにアクセスしようとする Ｂ社の従業がサーバＸに誘導される。求める答えはイとなる。

問165　ア

パスワードリスト攻撃に関する問題である。

アのパスワードリスト攻撃は、ネットサービスやコンピュータシステムの利用者アカウントの乗っ取りを試みる攻撃手法の一つで、別のサービスやシステムから流出したアカウント情報を用いてログインを試みる手法である。脆弱なサービスやシステムが攻撃者の侵入を受け、利用者のアカウント名とパスワードのリスト一覧の情報が流出すると、その情報を利用して別のシステムへの攻撃を試みるのがパスワードリスト攻撃で、同じアカウント名とパスワードを使っている利用者のアカウントでログインし、利用者になりすまして不正に操作することができてしまう。求める答えはアとなる。

イのブルートフォース攻撃は、暗号やパスワードを解読、解析するための手法のひとつで、特定のユーザＩＤに対して考えられる全ての暗号鍵を自動化されたプログラムによってひたすら入力し、復号化プログラムによって、暗号が意味のある文字列になるかどうかを試行錯誤しながら調べて行く方法である。

ウのリバースブルートフォース攻撃は、不正ログインを目的とするアカウント突破手法で、特定のパスワードに対して、ユーザーＩＤに使用され得る文字列の組み合わせを用いて総当り的にログインを試みる手法のことである。

エのレインボー攻撃は、想定されうるパスワードとそのハッシュ値との対のリストを用いて、入手したハッシュ値からパスワードを効率的に解析する手法である。

問166　ア

ブルートフォース攻撃に関する問題である。

ブルートフォース攻撃は、暗号解読手法の一つで、考えられる全ての鍵をリストアップし、片っ端から解読を試みる方式である。暗号文の一部を復号プログラムにしたがって変換し、意味のある文章になるか調べる。どのような形態の暗号に対しても攻撃できるが、鍵の長さが増えると考えられる鍵のパターンの数は幾何級数的に増大するため、効率の悪い攻撃手法である。

アはブルートフォース攻撃、イは線形解読法、ウは関連鍵攻撃、エは差分解読法である。求める答えはアとなる。

問167　ウ

サイバーセキュリティ経営ガイドラインに関する問題である。

経営者が留意すべき事項、セキュリティ責任者が指示すべき事項について、次の１０重要項目をまとめている。

① サイバーセキュリティリスクの認識、組織全体での対応の策定
② サイバーセキュリティリスク管理体制の構築
③ サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
④ サイバーセキュリティ対策フレームワーク構築と対策の開示
⑤ 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施および状況把握
⑥ サイバーセキュリティ対策のための資源確保(予算、人材等)
⑦ ＩＴシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
⑧ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
⑨ 緊急時の対応体制の整備、定期的かつ実践的な演習の実施
⑩ 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

以上の１０項目の内容は、自社のセキュリティ対策と系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施および状況把握に関するものである。

アはユーザ、イは株主、ウは系列企業やサプライチェーンのビジネスパートナー、エは地域社会である。求める答えはウとなる。

問168　ウ

タイムスタンプサービスに関する問題である。

タイムスタンプは、タイムスタンプに刻印されている時刻以前にその電子文書が存在していたこと（存在証明）と、その時刻以降、当該文書が改ざんされていないこと（非改ざん証明）を証明するものである。

アは標準時配信サービス、イはバイオメトリックス認証、ウはタイムスタンプサービス、エはＮＴＰである。求める答えはウとなる。

問169　ウ

公開鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。

イのKCipher-２は、九州大学とＫＤＤＩ研究所により共同開発されたストリーム暗号で、共通鍵暗号方式ある。

ウのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。求める答えはウとなる。

エのＳＨＡ-２５６は、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順である。

問170　ア

ボットネットに関する問題である。

ボットネットは、パソコンやスマートフォンを第三者の指示通りに動くロボットにしてしまう悪意のあるプログラムであり、そのボットをいくつも集めてネットワーク化したものがボットネットである。Ｃ＆Ｃサーバーは、マルウェアに感染したボットネットに指令を送り、制御の中心となるサーバーである。

Ｃ＆Ｃサーバの役割は、ボットネットの遠隔操作が可能なマルウェアに情報収集及び攻撃活動を指示するであり、求める答えはアとなる。

問171　エ

ワームとトロイの木馬に関する問題である。

ワームはコンピュータウィルスの一種で、ネットワークやＵＳＢメモリなどを感染経路にして自己増殖し、システムに害を与える悪質なコンピュータプログラムである。ワーム自体は破壊を行わないが、増殖を繰り返していくことでコンピュータのＣＰＵの処理やディスクの容量などを占有し、システムに負荷をかけたり、停止させたりする。

トロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、データの破壊、改ざんなどの不正行為を実行させるウィルスで、ファイルを削除してしまう機能を持ったプログラムを作る。利用者がプログラムを起動すると、ファイルが勝手に削除されてしまう。

アはランサムウェアの特徴、イはマルウェアの特徴、ウはトロイの木馬の特徴、エはワームの特徴である。求める答えはエとなる。

問172　イ

リスクアセスメントに関する問題である。

リスクアセスメントはリスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク特定は、リスクを発見し、認識し、記述するプロセスである。リスク分析は、リスクの特質を理解し、リスクレベルを決定するプロセスである。リスク評価は、リスクが受容可能か許容可能かを決定するためにリスク分析の結果をリスク基準と比較するプロセスである。

リスクアセスメントはリスク管理プロセス内のサブプロセスである。安全工学上のリスクは、人、環境、物に悪い影響をあたえる可能性と大きさ(の積)である。予測されるリスクの可能性と大きさ(予測値)と、許容されるリスクの可能性と大きさ(許容値)を比較し、予想値が許容値を上回った時リスク軽減の施策又はリスク回避の施策をとるという意思決定を行い、実際にその施策をとり、より安全な状態を実現するプロセスをとることになる。このプロセス全体がリスク管理プロセスである。リスクアセスメントはリスク管理プロセス内の意思決定サブプロセスとなる。

リスクアセスメントを構成するプロセスの組み合わせは、リスク特定、リスク分析、リスク評価である。求める答えはイとなる。

問173　ウ

ＣＳＩＲＴに関する問題である。

ＣＳＩＲＴ(シーサート)は、コンピュータセキュリティにかかるインシデントに対処するための組織の総称で、インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をしいる。シーサートの活動は、目的、立場、活動範囲、法的規制などの違いからそれぞれ独自で活動を行ってきた。 しかし、コンピュータセキュリティインシデントの攻撃が巧妙かつ複雑になり、迅速な対応には、単独のシーサートでは困難な状況になってきている。日本国内の企業事情を巧みに利用した攻撃手法などによるコンピュータセキュリティインシデントや、対応ノウハウの蓄積が難しい標的型攻撃などの存在があり、インターネットの発達、ビジネスにおけるＩＴへの依存度の高まりから、コンピュータセキュリティインシデントの発生リスクも大幅に高まり、攻撃が単なる愉快犯から、経済的利益を目的とした犯行へと移り変わっており、その手法も高度化、複雑化し、問題の把握がより難しくなる傾向にある。これらに適切に対処するためには､同じような状況や課題を持つシーサート同士による緊密な連携と、インシデント関連情報、脆弱性情報、攻撃予兆情報などを互いに収集し、積極的に共有する必要があり、互いに協調し、高いレベルでの緊密な連携体制の実現を目指し、共通の問題を解決する場を設けることを目的とした日本シーサート協議会が設立された。

アはＩＣＡＮＮ、イはＩＥＴＦ、ウはＣＳＩＲＴ、エはハクティビストである。求める答えはウとなる。

問174　エ

SMTP-AUTHに関する問題である。

アのAPOPは、POP3は利用者がメールサーバにユーザ名とパスワードをそのまま送信するため、通信途上に悪意の第三者がいる場合､容易にパスワードを盗まれてしまうという問題があったが、APOPではハッシュ関数などを用いてパスワードを暗号化して送受信することにより、容易に盗聴できないようにすることができる。

イのPOP3Sは、POP3による接続前にSSL/TLSで伝送路を暗号化するもので、メールや添付ファイルのデータだけでなくPOP3では平文で送受信されていたユーザ名とパスワードも暗号化されるため、盗聴によるアカウント乗っ取りなどの危険も低くなる。

ウのS/MIMEは、電子メールソフトのために暗号技術を使って、認証、通信文の完全性、発信元の否認防止、プライバシーとデータの機密保護などのセキュリティ機能を提供する。

エのSMTP-Authは、メールクライアントからSMTPサーバへメールの送信依頼を行う際に認証過程を導入し、クライアント側にアカウント名やパスワードを申告させて確かに正規の利用者であることを確認してから送信を受け付けるようにする認証方法である。求める答えはエとなる。

問175　エ

ドライブバイダウンロード攻撃に関する問題である。

ドライブバイダウンロード攻撃は、Ｗｅｂブラウザを通じて、ユーザーに気づかせないようにソフトウェア部品をダウンロードさせることである。この手法は、スパイウェアやマルウェア、コンピュータウィルスなどが侵入・攻撃を行う場合の経路として用いられる。ユーザーがＷｅｂサイトを閲覧しただけで自動的にスパイウェアやマルウェアがダウンロードされてしまったり、

ダウンロードが実行されてもユーザーは気づくことができなかったり、というに特徴がある。また、企業のＷｅｂサイトが改ざんされ、ドライブバイダウンロードが埋め込まれてユーザーを脅かした例もある。ドライブバイダウンロードによる攻撃は、主にＷｅｂブラウザやＯＳの脆弱性を突くようにして行われる。そのため、ドライブバイダウンロードによる攻撃を回避するためには、ウィルス対策ソフトやファイアーウォールの導入などを並んで、ＷｅｂブラウザやＯＳのセキュリティパッチを更新して常に最新の状態に保つといった事柄が主要な施策となる。

アはランサムウェア、イはルートキット攻撃、ウはＳＱＬインジェクション、エはドライブバイダウンロードである。求める答えはエとなる。

問176　イ

公開鍵暗号方式に関する問題である。

公開鍵暗号方式は通信文を送信する場合、送信元で公開鍵により暗号化し、受信先で専用の秘密鍵で復号する方式である。暗号化する鍵と復号する鍵が異なり、片方の鍵を公開し、もう一方の鍵は秘密にした暗号化方式である。代表的なものにＲＳＡ方式がある。公開鍵から秘密鍵を発見することは不可能であり、公開鍵を管理する必要がない。秘密鍵は自分だけが持てばよいので、鍵管理が簡単で安全度が高い。論理が複雑なため処理時間が長くなり、処理速度は共通鍵方式よりも遅い。公開鍵暗号を守秘に使う場合、送信者は受信者の公開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、元の平文を得ることができる。鍵の配布やデジタル署名に利用される。

ＡさんがＢさんの公開鍵で暗号化した電子メールであるから、この暗号文を平文に復号できるはＢさんの秘密鍵だけである。従って、Ｂさんだけが自信の秘密鍵で復号できるが適切である。求める答えはイとなる。

問177　ア

真正性に関する問題である。

情報セキュリティの７特性である機密性、完全性、可用性、真正性、責任追跡性、否認防止、信頼性に関係する問題である。

アの真正性は、ある主体または資源が、主張通りであることを確実にする特性である。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。求める答えはアとなる。

イの信頼性は、意図した動作および結果に一致する特性である。

ウの責任追跡性は、あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性である。

エの否認防止は、ある活動または事象が起きたことを、後になって否認させないように証明する能力である。

問178　ウ

ポストスキャンに関する問題である。

ポートスキャンは攻撃の前段階の調査として行われるもので、当該コンピュータの各ポートへ接続開始を要請するデータを送り、どのような反応を返すかを確かめる。これにより、アクセス

を受け付けているポートが何番か、どのようなソフトウェアが使用されているか、ソフトウェアの設定がどのようになっているかなどを外部からある程度知ることができ、攻撃に利用可能な設定の不備やソフトウェアの脆弱性などがないかを調べることができる。ポートスキャンは攻撃者が攻撃対象に対して行う場合のほかに、コンピュータやネットワークの管理者などが自らが管理・運用するコンピュータにセキュリティ上の問題がないか調べるために実行することもある。

事前調査の段階において、攻撃できそうなサービスがあるかどうかを調査することである。求める答えはウとなる。

アの後処理段階、イの権限取得段階、エの不正実行段階は適切でない。

問179　ウ

パケットフィルタリングに関する問題である。

通信を行う場合、通信前にポート番号を決める必要がある。通常、ポート番号はアプリケーションごとに標準で決められた番号があり、０～１０２３の番号が割り当てられている。インターネット上のＳＭＴＰサーバと通信を行う場合はサーバ側のポート番号は２５を用いる。

この問題では、社内のＰＣからインターネット上のＳＭＴＰサーバにアクセスする場合であるから、ＳＭＴＰサーバでのポート番号は２５、ＰＣのポート番号は１０２４以上を用いる。

ＰＣからの発信は、送信元はＰＣ、あて先はＳＭＴＰサーバ、送信元ポート番号１０２４以上、あて先ポート番号２５であり、サーバからの応答は、送信元はＳＭＴＰサーバ、あて先はＰＣ、送信元ポート番号２５、あて先ポート番号１０２４以上となる。求める答えはウとなる。

問180　エ

セキュリティバイデザインに関する問題である。

セキュア・バイ・デザインは、システムやソフトウェアの企画・設計、開発の段階からセキュリティ対策を組み込む考え方のことである。昨今のサイバー攻撃は企業等に大きな損失を与える可能性があることが認識されるようになり、運用時だけでなく、システムやソフトウェアの設計や開発段階で、セキュリティ対策を考慮する「セキュア・バイ・デザイン」の考え方に注目が集まっている。「セキュア・バイ・デザイン」を実現するための技術や手法には、プログラムの実行状態やソースコードを解析・検証する「プログラム解析」や、システムやアプリケーションなどの複数のコンポーネント間の通信プロトコルの正しさを検証する「プロトコル検証」といった様々なものがある。標的型攻撃などのように、特定のターゲットに対し、周到に、時間をかけて準備され、継続的に実行されるサイバー攻撃に対応していくためには、様々な観点からセキュリティを考え、対策を実施することが重要である。「セキュア・バイ・デザイン」はその対策の一つとして、システムの運用段階で実施される各種セキュリティ対策と併せて実施していく必要がある。求める答えはエとなる。

問181　イ

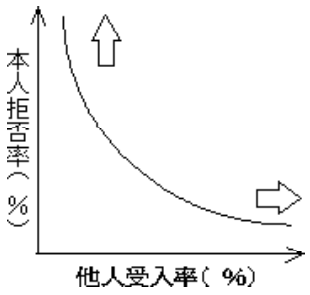
生体認証システムに関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。

ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を

重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。

生体認証システムを導入する場合、本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する必要がある。求める答えはイとなる。



問182　イ

ＳＰＦの仕組みに関する問題である。

ＳＰＦは､電子メールの送信元ドメインが詐称されていないかを検査するための仕組みである。インターネットでメール送信に使用されるＳＭＴＰは 差出人のメールアドレスを自由に設定することが可能で、 送信元を偽った「なりすましメール」を簡単に送ることができる。ＳＰＦは、こうしたメールアドレスにおけるなりすましを防ぐための技術の一つで、ＤＮＳを利用するのが特徴である。ドメインをＳＰＦに対応させるために、そのドメインのゾーンデータにＳＰＦレコードという情報を追加し、ＳＰＦレコードに、そのドメイン名を送信元としてメールを送ってもよいサーバのＩＰアドレス等を記述する。一方、ＳＰＦに対応したメール受信サーバは、メールの受信時にそのメールの送信元となっているドメインのＳＰＦレコードを、ＤＮＳで問い合わせる。送信元のサーバがＳＰＦレコード中で許可されていない場合は、送信ドメインの詐称が行われたと判断して、受信を拒否するなどの処理を行う。つまりＳＰＦは、送信元サーバのＩＰアドレスとＤＮＳを利用して、あらかじめ想定された送信元以外からのなりすましメールを検出できるようにする機構である。

アのディジタル証明書を利用したものではない。

イの送信元のドメイン情報と送信したサーバのＩＰアドレスを利用して確認する仕組みはＳＰＦである。求める答えはイとなる。

ウの送信者の上司の承認による確認ではない。

エのＳＰＦはすべての電子メールをアーカイブすることではない。