gzn030401 「セキュリティとリスク管理」解答解説

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　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49　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　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55　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56　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57　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ー要求事項」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58　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59　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60　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61　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62　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63　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64　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65　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66　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67　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68　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69　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70　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71　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72　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73　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74　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75　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76　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77　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78　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79　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80　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81　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。