２．コンピュータの技術要素

２．３情報セキュリティ（情報セキュリティの脅威（１））

問題１

　“情報セキュリティの脅威”における分類に関する説明のうち、適切でないものはどれか。

ア．機器自体や機器が設定された建物などに関する脅威を、物理的脅威と呼ぶ。

イ．コンピュータ技術を利用して攻撃してくる脅威を、技術的脅威と呼ぶ。

ウ．組織に対して経済的な損失を与える脅威を、経済的脅威と呼ぶ。

エ．人間の行為が原因となる脅威を、人的脅威と呼ぶ。

問題２

　システムの正当な利用者が処理をうっかり間違えた結果として、重要なデータが消去されてしまった。

このような脅威を何というか。

ア．誤操作　　　イ．破壊　　　　ウ．破損　　　　エ．紛失

問題３

　悪意をもって他人のPCに侵入し、データを盗み見たり、破壊したりする行為を何というか。

ア．クラッキング　　　　 　 　　　　 イ．ショルダハッキング

ウ．トラッキング　　　 　 　　　　　エ．標的型攻撃

問題４

セキュリティ事故の例のうち、原因が物理的脅威に分類されるものはどれか。

ア．大雨によってサーバ室が浸水し、機器が停止した。

イ．外部から公開サーバに大量のデータを送られ、公開サーバが停止した。

ウ．攻撃者がネットワークを介して社内のサーバに侵入し、ファイルを破壊した。

エ．社員が電子メールの宛先を間違えて、重要なデータが流出した。

問題５

　情報システムの安定稼働を妨げるさまざまな脅威への事前対策に関する記述のうち、適切なものはどれか。

ア．外部からの不正侵入を完全に阻止できれば、不正アクセスへの事前対策としては問題ない。

イ．自然災害に対しては予備が困難なので、人的災害に絞って事前対策を講じる。

ウ．すべてのデータをバックアップしておけば、ほかの事前説明は不要となる。

エ．予想損失や対策コストとのトレードオフを考慮して、必要な事前対策を講じる。

問題６

　ソーシャルエンジニアリングによる被害に結びつきやすい状況はどれか。

ア．運用担当者のセキュリティ意識が低い。

イ．サーバ室の天井の防水対策が行われていない。

ウ．サーバへのアクセス制御が行われていない。

エ．通信経路が暗号化されていない。

問題７

　PCやハードディスクを譲渡したり返却したりする前に実施しておくこととして、ハードディスクからの情

報漏えいを防ぐ最も確実な方法はどれか。

ア．ハードディスク全体を16進数の00やFF、または乱数で複数回上書きしておく。

イ．ハードディスク全体を倫理フォーマットしておく。

ウ．ハードディスク内のすべてのファイルやフォルダをごみ箱に捨て、最後にごみ箱を空にしておく。

エ．ハードディスクにパスワードロックをかけておく。

２．３情報セキュリティ（情報セキュリティの脅威（２））

問題１

　悪意をもって作成されたソフトウェアの総称はどれか。

ア．アドウェア　　　　　 　 　　　　 イ．シェアウェア

ウ．マルウェア　　　　 　 　　　　　エ．ミドルウェア

問題２

　マイクロウィルスに関する説明として、適切なものはどれか。

ア．インターネットなどのネットワークを通じて、感染したコンピュータを外部から不正に遠隔操作できる

ようにする。

イ．個人情報などを盗み出して、第三者に自動的に送信する。

ウ．便利なソフトウェアに見せかけてインストールさせた後、不正な動作をする。

エ．ワープロソフトや表計算ソフトのデータファイルに感染する。

問題３

銀行やクレジットカード会社などを装った偽のWebページを開設し、金融機関や公的機関などを装った偽の電子メールなどで、利用者の巧みに誘導して、暗証番号やクレジットカード番号などの個人情報を盗み取る行為を何と呼ぶ。

ア．キーロガー　　　　　 　 　　　　 イ．ゼロデイ攻撃

ウ．バッファオーバーフロー攻撃 　　　エ．フィッシング

問題４

スパムメールの説明として、適切なものはどれか。

ア．あらかじめ登録した参加者全員に配信される。同じ内容の電子メールのこと。

イ．受信者の承諾なしに無差別に送付される電子メールのこと。

ウ．受信を許諾した相手にだけ送信される電子メールのこと。

エ．電子メールの受信者が複数の相手に同一内容の電子メールの送信や転送を行い、受信者が増加し続ける

電子メールのこと。

問題５

　ランサムウェアの説明として、適切なものはどれか。

ア．ウイルスなどを検知して、コンピュータを脅威から守り、安全性を高めるソフトウェアの総称

イ．感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、

元に戻すための代金を利用者に要素するソフトウェア。

ウ．キーボード入力や画面出力といった入出力機能や、ディスクやメモリの管理などコンピュータシステム

全体を管理するソフトウェア

エ．ローマ字から平仮名や片仮名へ変換したり、仮名から漢字へ変換するなどコンピュータでの利用者の文

入力を補助するソフトウェア

問題６

DoS攻撃によって、サーバが受ける直接的な被害はどれか。

ア．暗号化してあるデータが解読される。

イ．管理者用パスワードが変更される。

ウ．コンピュータウイルスに感染する。

エ．サービスの提供が阻害される。

問題７

クロスサイトスクリプティングに関する記述として、適切なものはどれか。

ア．Webサイトの運営者が意図しないスクリプトを含むデータであっても、利用者のブラウザに送ってしま

う脆弱性を利用する。

イ．Webページの入力項目にOSの操作コマンドを埋め込んでWebサーバに送信し、サーバを不正に操作

する。

ウ．複数のWebサイトに対して、ログインIDとパスワードを同じものに設定するという利用者の習性を悪

用する。

エ．利用者の罠のあるWebサイトに誘導する目的などのために、偽の送信元IDアドレスをもったパケット

を送る。

２．３情報セキュリティ（情報セキュリティ管理）

問題１

　情報セキュリティの文書を詳細化の順に、

①

右の図のように上から並べた場合、①～③

に当てはまる用語の組合せとして、適切な

②

ものはどれか。

③

|  |  |  |  |
| --- | --- | --- | --- |
|  | ① | ② | ③ |
| ア | 基本方針 | 対策基準 | 対策実施手順 |
| イ | 基本方針 | 対策実施手順 | 対策基準 |
| ウ | 対策基準 | 基本方針 | 対策実施手順 |
| エ | 対策基準 | 対策実施手順 | 基本方針 |

問題２

　情報セキュリティにおける“可用性”の説明として、適切なものはどれか。

ア．システムの動作と出力結果が意図したものであること

イ．情報が正確であり、改ざんされたり破壊されたりしていないこと

ウ．許可された利用者が、必要なときに情報をアクセスできること

エ．許可されていないプロセスに対して、情報を非公開にすること

問題３

ISMSの運用において、監査結果をインプットとし、ISMSを継続的に改善するための是正処置及び予防処置を行うプロセスはPDCAサイクルのどれにあたるか。

ア．Ｐ　　　　　イ．Ｄ　　　　　ウ．Ｃ　　　　　エ．Ａ

問題４

リスクマネジメントにおいて、リスクを資産ごとに洗い出すものはどれか。

ア．リスク対策　イ．リスク特定　ウ．リスク評価　エ．リスク分析

問題５

　組織で策定する情報セキュリティポリシに関する記述のうち、最も適切なものはどれか。

ア．情報セキュリティ基本方針だけでなく、情報セキュリティに関する規則や手順の策定も経営者が行うべきである

イ．情報セキュリティ基本方針だけでなく、情報セキュリティに関する規則や手順の策定も社外に公開する

ことが求められる。

ウ．情報セキュリティに関する規則や手順は組織の状況にあったものにすべきであるが、最上位の情報セキ

ュリティ基本方針は業界標準の雛形をそのまま採用することが求められる。

エ．組織内の複数の部門で異なる情報セキュリティ対策を実施する場合でも、情報セキュリティ基本方針は

組織全体で統一させるべきである。

問題６

　組織の活動に関する記述ａ～dのうち、ISMSの特徴として、適切なものだけを全てあげたものはどれか。

ａ．一過性の活動ではなく改善と活動を継続する。

ｂ．現場が主導するボトムアップ活動である。

ｃ．導入及び活動は経営層を頂点とした組織的な取組みである。

ｅ．目標と期限を定めて活動し、目標達成によって終了する。

ア．ａ，ｂ　　　イ．ａ，ｃ　　　ウ．ｂ，ｄ　　　エ．ｃ，ｄ

問題７

　ISMSにおけるセキュリティリスクへの対応には、リスク移転、リスク回避、リスク受容及びリスク低減がある。リスク回避に該当する事例はどれか。

ア．セキュリティ対策を行って、問題発生の可能性を下げた。

イ．問題発生時の損害に備えて、保険に入った。

ウ．リスクが小さいことを確認し、問題発生時は損害を負担することにした。

エ．リスクの大きいサービスから撤退した。

２．３情報セキュリティ（情報セキュリティ対策）

問題１

　社内の情報セキュリティ教育に関する記述のうち、適切なものはどれか。

ア．再教育は、情報システムを入れ替えたときだけ実施する。

イ．新入社員へは、業務に慣れた後に実施する。

ウ．対策は、情報資産にアクセスする社員だけにする。

エ．内容は、社員の担当業務、役割及び責任に応じて変更する。

問題２

　バイオメトリクス認証の例として、適切なものはどれか。

ア．本人だけが知っているパスワードで認証する。

イ．本人だけがもっている身分証明書で認証する。

ウ．本人の指紋で認証する。

エ．ワンタイムパスワードを用いて認証する。

問題３

　ウイルス対策ソフトの適切な運用方法はどれか。

ア．インストールした時に一度だけ、ハードディスク全体を検査する。

イ．ウイルス対策ソフトは、ウイルス検査を行うときにだけ起動する。

ウ．導入後もウイルス定義ファイルの更新を継続して行う。

エ．プロバイダ側でウイルスチェックが行われている場合は、PCへのウイルス対策ソフトの導入は不要で

ある。

問題４

　プログラムによる自動投稿を防止するために、画面に表示された歪んだ文字や数字を入力させる仕組みはど

れか。

ア．画像認証（CARTCHA） 　　　　 イ．コンテンツフィルタ

ウ．電子透かし　　　　 　 　　　　　エ．バイオメトリクス認証

問題５

セキュリティ対策の目的①～④のうち、適切なアクセス権を設定することによって効果があるものだけを全て挙げたものはどれか。

①DoS攻撃から守る。

②情報漏えいを防ぐ。

③ショルダハッキングを防ぐ。

④不正利用者による改ざんを防ぐ。

ア．①，②　　　イ．①，③　　　ウ．②，④　　　エ．③，④

問題６

　生体認証による入退室管理システムに全社員を登録し、社内の各部屋に入室を許可する社員を設定した。

退室は管理していない。a～dの記述のうち、この入退室管理システムで実現できることだけを全て挙げたものはどれか。

①権限のある社員だけに入室を許可する。

②入室者が部屋にいた時間を記録する。

③入室を試みて、拒否された社員を記録する。

④部屋にいる人数を把握する。

ア．①，②，③　イ．①，③　　　ウ．①，④　　　エ．②，③，④

問題７

　インターネットでショッピングサイトに接続したとき、ブラウザにSSL鍵マークが表示された。さらに、サーバ証明書が、目的のショッピングサイトの運営者のものであることを確認した。このときに判断できることはどれか。

ア．このショッピングサイト運営者の財務状況は、安定している。

イ．このショッピングサイトで注文した商品は、納品目ウイルス対策ソフトは、ウイルス検査を行うときにだけ起動する。

ウ．利用者が入力した個人情報などが改ざんされても、サーバ側で修正できる。

エ．利用者が入力した個人情報などは、途中経路で漏えいすることはない。

２．３情報セキュリティ（アクセス制御）

問題１

パスワードに関する記述のうち、適切なものはどれか。

ア．パスワードには、英単語など意味のある言葉を使用する。

イ．パスワードは必ずメモしておき、誰からも見やすい場所に貼っておく。

ウ．パスワード漏えいの事実が発覚した場合、速やかに管理者に報告する。

エ．忘れないようにするために、できるだけ短いパスワードを設定する。

問題２

一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組みを何というか。

ア．シングルサインオン　　 　　　　 イ．ディジタルフォレンジックス

ウ．バイオメトリクス認証 　　　　　エ．ワンタイムパスワード

問題３

ネットワークにおいて、外部からの不正アクセスを防ぐために内部ネットワークと外部ネッワークの間に置

かれるものはどれか。

ア．DNSサーバ　　　 　　 　　　　 イ．サーチエンジン

ウ．スイッチングハブ　　 　　　　　エ．ファイアウォール

問題４

セキュリティに問題があるPCを社内ネットワークなどに接続させないことを目的とした仕組みであり、外

出先で使用したPCを会社に持ち帰った際に、ウイルスに感染していないことなどを確認するために利用するものはどれか。

ア．DMZ　　　　　　 　　 　　　　 イ．IDS

ウ．検疫ネットワーク　　 　　　　　エ．ファイアウォール

問題５

システムの利用者認証技術に関する記述のうち、適切なものはどれか。

ア．一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組みをチャレンジレスポンス認証という。

イ．指紋や声紋など、身体的な特徴を利用して本人認証を行う仕組みをシングルサインオンという。

ウ．特定の数字や文字の並びではなく、位置についての情報を覚え、認証時には画面に表示された表の中で、

自分が覚えている位置に並んでいる数字や文字をパスワードとして入力する方式をバイオメトリクス認証

という。

エ．認証のために一度しか使えないパスワードのことを、ワンタイムパスワードという。

問題６

企業内ネットワークからも、外部ネットワークからも論理的に隔離されたネットワーク領域であり、そこに

設定されたサーバが外部から不正アクセスを受けたとしても、企業内ネットワークには被害が及ばないように

するためのものはどれか。

ア．DMZ　　　　イ．DNS　　　　ウ．DoS　　　　エ．SSL

問題７

無線LANのセキュリティにおいて、アクセスポイントが接続要求を受け取ったときに、端末固有の情報固有の情報を基にアクセス制御を行う仕組みはどれか。

ア．ESSID　　　　　　　　 　　　　 イ．MACアドレスフィルタリング

ウ．WEP　　　　　　　　　 　　　　 エ．WPA

２．３情報セキュリティ（暗号化／ディジタル署名）

問題１

共通鍵暗号方式に関する記述のうち、適切なものはどれか。

ア．暗号化に用いる鍵を第三者に公開しても、第三者は暗号文を復号できない。

イ．公開鍵暗号方式よりも、暗号化処理と復号処理の計算量は少ない。

ウ．通信経路で改ざんされた暗号文を復号処理で訂正し、元の暗号文に復元する機能をもつ。

エ．複数の相手ごとに通信内容を秘密にしたい場合でも、暗号化に用いる鍵は一つである。

問題２

無線LANで利用される暗号方式の規格はどれか。

ア．AES　　　　イ．DES　　　　ウ．RSA　　　　エ．WPA2

問題３

Xさんは、Yさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にす

る必要があるので、公開鍵暗号方式を用いて暗号化して送信したい。電子メールの内容を暗号化するのに使用

する鍵はどれか。

ア．Xさんの公開鍵 　 　　 　　　　 イ．Xさんの秘密鍵

ウ．Yさんの公開鍵　　　 　　　　　エ．Yさんの秘密鍵

問題４

公開鍵基盤（PKI）における認証局（CA）が果たす役割はどれか。

ア．SSLを利用した暗号化通信で使用する認証プログラムを提供する。

イ．Webサーバに不正な仕組みがないことを示す証明書を発行する。

ウ．公開鍵が被認証者のものであることを示す証明書を発行する。

エ．被認証者のディジタル署名を安全に送信する。

問題５

セション鍵暗号方式で用いられるハイブリッド方式に関する記述のうち、適切なものはどれか。

ア．共通鍵と公開鍵で二重に暗号化するので、改ざんが難しい。

イ．共通鍵と公開鍵を併用するので、高速な暗号通信には向かない。

ウ．公開鍵暗号方式を使って、共通鍵を暗号化して通信相手に送信する。

エ．使用する鍵の数は、全体で単独方式の2乗倍必要となる。

問題６

受信した電子メールにPKI（公開鍵基盤）を利用してディジタル署名を付与した場合に関する記述①～④の

うち、判断可能な記述だけをすべて挙げたものはどれか。

①電子メールの添付ファイルはウイルスに感染していない。

②電子メールの内容は通信途中において、他の誰にも盗み見られていない。

③電子メールの発信者は、なりすましされていない。

④電子メールは通信途中で改ざんされていない。

ア．①，②　　　イ．①，③　　　ウ．②，④　　　エ．③，④

問題７

小文字の英字からなる文字列の暗号化を考える。次表の英字を文字番号に変換し、変換後の文字番号につい

て1文字目には1を、2文字目には2を、…、ｎ文字目にはｎを加える。それぞれの数を26で割った余りを

新たに文字番号とみなし、表から対応する英字に変換する。

例　fax → 6、24 → 6+1、1+2、24+3 → 7、3、27 → 7、3、27 → 7、3、27 → 7、3、1 → gca

この手続きで暗号化した結果が”tmb”であるとき、元の文字列はどれか。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 文字番号 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 英字 | a | b | c | d | e | f | g | h | i | j | k | l | m |
| 文字番号 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 英字 | n | o | p | q | r | s | t | u | v | w | x | y | z |

ア．she　　　イ．shy　　　ウ．ski　　　エ．sky