情報セキュリティマネジメント試験合格講座

情報セキュリティマネジメント試験対策

模擬試験・予想問題

午前問題（50 問）

［問1］情報セキュリティの観点から、システムの可用性を高める施策の例として、最も適切なものはどれか。

ア　生体認証を採用する。
イ　ディジタル署名を行う。
ウ　データを暗号化する。
エ　ハードウェアを二重化する。

［問2］情報セキュリティの対策を、技術的セキュリティ対策、人的セキュリティ対策及び物理的セキュリティ対策の三つに分類するとき、物理的セキュリティ対策に該当するものはどれか。

ア　従業員と守秘義務契約を結ぶ。
イ　電子メール送信時にディジタル署名を付与する。
ウ　ノート PC を保管するときに施錠管理する。
エ　パスワードの変更を定期的に促す。

［問3］IC カードの耐タンパ性を高める対策はどれか。

ア　IC カードと IC カードリーダとが非接触の状態で利用者を認証して、利用者の利便性を高めるようにする。
イ　故障に備えてあらかじめ作成した予備の IC カードを保管し、故障時に直ちに予備カードに交換して利用者が IC カードを使い続けられるようにする。
ウ　信号の読み出し用プローブの取付けを検出すると IC チップ内の保存情報を消去する回路を設けて、IC チップ内の情報を容易に解析できないようにする。
エ　退職者の IC カードは業務システム側で利用を停止して、ほかの利用者が使用できないようにする。

［問4］ISMS に関する記述のうち、適切なものはどれか。

ア　ISMS のマネジメントサイクルは、セキュリティ事故が発生した時点で開始し、セキュリティ事故が収束した時点で終了する。
イ　ISMS の構築、運用は、組織全体ではなく、必ず部門ごとに行う。
ウ　ISMS を構築する組織は、保護すべき情報資産を特定し、リスク対策を決める。
エ　情報セキュリティ方針は、具体的なセキュリティ対策が記述されたものである。

［問5］ISMS の情報セキュリティ方針に関する記述として、適切なものはどれか。

ア　情報セキュリティ方針は、トップマネジメントが確立しなければならない。
イ　情報セキュリティ方針は、社外に公表してはならない。
ウ　一度制定した情報セキュリティ方針は変更できない。
エ　個人情報や機密情報を扱わない従業者には、情報セキュリティ方針を周知しなくてもよい。

［問6］社員に対する情報セキュリティ教育の実施に関する記述 a～d のうち、適切なものだけを全て挙げたものはどれか。

a 情報セキュリティ違反をした者に対する再教育に当たっては、同じ過ちを繰り返さないための予防処置も含める。
b 新入社員に対する研修プログラムに組み込む。
c 対象は情報システム部門に所属する社員に限定する。
d 定期的な実施に加えて、情報セキュリティに関わる事件や事故が発生した後にも実施する。

ア　a、b、d
イ　a、c、d
ウ　a、d
エ　b、c

［問7］リスク対策をリスクコントロールとリスクファイナンスに分けた場合、リスクファイナンスに該当するものはどれか。

ア　システムが被害を受けた場合を想定して保険をかけた。
イ　システム被害につながるリスクの発生を抑える対策に資金を投入した。
ウ　システムを復旧するのに掛かった費用を金融機関から借り入れた。
エ　リスクが顕在化した場合のシステム被害を小さくする対策に資金を投入した。

［問8］リスクマネジメントを推進するために、リスクマネジメントシステムの実行計画を最初に策定した。その後に行う活動を次の a～c に分けて行うとき、PDCA サイクルに従った実施順序として、適切なものはどれか。

a 実行計画に従ってリスク対策を実施する。
b 実施の効果を測定し、リスクマネジメントシステムの有効性を評価する。
c リスクマネジメントシステムに関する是正・改善措置を実施する。

ア a→b→c
イ a→c→b
ウ c→a→b
エ c→b→a

［問9］CSIRT の説明として、適切なものはどれか。

ア IP アドレスの割当て方針の決定、DNS ルートサーバの運用監視、DNS 管理に関する調整などを世界規模で行う組織である。
イ インターネットに関する技術文書を作成し、標準化のための検討を行う組織である。
ウ 国レベルや企業・組織内に設置され、コンピュータセキュリティインシデントに関する報告を受け取り、調査し、対応活動を行う組織の総称である。
エ 情報技術を利用し、信教や政治的な目標を達成するという目的をもった人や組織の総称である。

［問10］ネットワーク障害の原因を調べるために、ミラーポートを用意して、LAN アナライザを使用するときに留意することはどれか。

ア LAN アナライザがパケットを破棄してしまうので、測定中は測定対象外のコンピュータの利用を制限しておく必要がある。
イ LAN アナライザに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。
ウ 障害発生に備えて、ネットワーク利用者に LAN アナライザの保管場所と使用方法を周知しておく必要がある。
エ 測定に当たって、LAN ケーブルを一時的に切断する必要があるので、利用者に対して測定日を事前に知らせておく必要がある。

［問11］無線 LAN のセキュリティを向上させるための対策はどれか。

ア　ESSID をステルス化する。
イ　アクセスポイントへの電源供給は LAN ケーブルを介して行う。
ウ　通信の暗号化方式を WPA2 から WEP に変更する。
エ　ローミングを行う。

［問12］無線 LAN に関する記述として、適切なものだけを全て挙げたものはどれか。

a ESSID は、設定する値が無線 LAN の規格ごとに固定値として決められており、利用者が変更することはできない。
b 通信規格の中には、使用する電波が電子レンジの電波と干渉して、通信に影響が出る可能性のあるものがある。
c テザリング機能で用いる通信方式のひとつとして、使用されている。

ア　a
イ　a、b
ウ　b、c
エ　c

［問13］会社や団体が、自組織の従業員に貸与するスマートフォンに対して、セキュリティポリシに従った一元的な設定をしたり、業務アプリケーションを配信したりするなど、スマートフォンの利用状況などを一元管理する仕組みはどれか。

ア　BYOD(Bring Your Own Device)
イ　ECM(Enterprise Contents Management)
ウ　LTE(Long Term Evolution)
エ　MDM(Mobile Device Management)

［問14］スマートフォンを安全に利用するために行うこととして、適切なものはどれか。

ア　OS はアップデートせず、購入時の状態のままで利用する。
イ　権限昇格などの改造を行い、機能を強化する。
ウ　パスワードによる画面のロック機能を設定する。
エ　有用と思うアプリケーションであれば、どのような Web サイトからダウンロードしてもよい。

［問15］NIDS(ネットワーク型 IDS)を導入する目的はどれか。

ア　管理下のネットワーク内への不正侵入の試みを検知し、管理者に通知する。
イ　サーバ上のファイルが改ざんされたかどうかを判定する。
ウ　実際にネットワークを介してサイトを攻撃し、不正に侵入できるかどうかを検査する。
エ　ネットワークからの攻撃が防御できないときの損害の大きさを判定する。

［問16］迷惑メールの検知手法であるベイジアンフィルタリングの説明はどれか。

ア　信頼できるメール送信元を許可リストに登録しておき、許可リストにない送信元からの電子メールは迷惑メールと判定する。
イ　電子メールが正規のメールサーバから送信されていることを検証し、迷惑メールであるかどうかを判定する。
ウ　電子メールの第三者中継を許可しているメールサーバを登録したデータベースに掲載されている情報を基に、迷惑メールであるかどうかを判定する。
エ　利用者が振り分けた迷惑メールから特徴を学習し、迷惑メールであるかどうかを統計的に解析して判定する。

［問17］バイオメトリクス認証に関する記述として、適切なものはどれか。

ア　認証用データとの照合誤差の許容値を大きくすると、本人を拒否してしまう可能性と他人を受け入れてしまう可能性はともに小さくなる。
イ　認証用の ID やパスワードを記憶したり、鍵やカード類を携帯したりする必要がない。
ウ　パスワードやトークンなど、他の認証方法と組み合わせて使うことはできない。
エ　網膜や手指の静脈パターンは経年変化が激しいので、認証に使用できる有効期間が短い。

［問18］SQL インジェクション攻撃を防ぐ方法はどれか。

ア　入力から、上位ディレクトリを指定する文字列(../)を取り除く。
イ　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。
ウ　入力に HTML タグが含まれていたら、解釈、実行できないほかの文字列に置き換える。
エ　入力の全体の長さが制限を超えていたときは受け付けない。

［問19］クライアントと Web サーバの間において、クライアントが Web サーバに送信されたデータを検査して、SQL インジェクションなどの攻撃を遮断するためのものはどれか。

ア　SSL-VPN 機能
イ　WAF
ウ　クラスタ構成
エ　ロードバランシング機能

[問20] ワンタイムパスワードに関する記述中の a、b に入れる字句の適切な組合せはどれか。

利用者は、トークンと呼ばれる装置などを用いて生成された〔 a 〕のパスワードを使って認証を受ける。このパスワードをワンタイムパスワードと呼び、これを利用することで、パスワードの漏えいによる〔 b 〕のリスクを低減することができる。

ア a:固定 b:Dos 攻撃
イ a:固定 b:なりすまし
ウ a:使い捨て b:Dos 攻撃
エ a:使い捨て b:なりすまし

[問21] IDS の特徴のうち、適切なものはどれか。

ア ネットワーク型 IDS では、SSL を利用したアプリケーションを介して行われる攻撃を検知できる。
イ ネットワーク型 IDS では、通信内容の解析によって、ファイルの改ざんを検知できまる。
ウ ホスト型 IDS では、シグネチャとのパターンマッチングを失敗させるためのパケットが挿入された攻撃でも検知できる。
エ ホスト型 IDS では、到着する不正パケットの解析によって、ネットワークセグメント上の不正パケットを検知できる。

[問22] ファイルのあるレコードが変更されたときに、変更された内容を特定する方法として、適切なものはどれか。

ア ファイルのサイズ及び更新日時を記録しておく。
イ ファイルの複製をとっておき、後で照合する。
ウ レコードの件数をファイル内に記録しておく。
エ レコードをキー項目で昇順に並べておく。

［問23］総務省及び経済産業省が策定した「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」を構成する暗号リストの説明のうち、適切なものはどれか。

ア　推奨候補暗号リストとは、CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストである。
イ　推奨候補暗号リストとは、候補段階に格下げされ、互換性維持目的で利用する暗号技術のリストである。
ウ　電子政府推奨暗号リストとは、CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストである。
エ　電子政府推奨暗号リストとは、推奨段階に格下げされ、互換性維持目的で利用する暗号技術のリストである。

［問24］暗号方式には共通鍵暗号方式と公開鍵暗号方式がある。共通鍵暗号方式の特徴として、適切なものはどれか。

ア　暗号化通信する相手が 1 人のとき、使用する鍵の数は公開鍵暗号方式よりも多い。
イ　暗号化通信に使用する鍵を、暗号化せずに相手へ送信しても安全である。
ウ　暗号化や復号に要する処理時間は、公開鍵暗号方式よりも短い。
エ　鍵ペアを生成し、一方の鍵で暗号化した暗号文は他方の鍵だけで復号できる。

［問25］PKI において、電子証明書が正当性を証明しているものはどれか。

ア　暗号化アルゴリズム
イ　共通鍵
ウ　公開鍵
エ　秘密鍵

［問26］SPF を利用する目的はどれか。

ア　HTTP 通信の経路上での中間者攻撃を検知する。
イ　LAN への PC の不正接続を検知する。
ウ　内部ネットワークへの不正侵入を検知する。
エ　メール送信のなりすましを検知する。

［問27］不正アクセスを行う手段のひとつであるIPスプーフィングの説明として、適切なものはどれか。

ア　金融機関や有名企業などを装い、電子メールなどを使って利用者を偽のサイトへ誘導し、個人情報などを取得すること
イ　侵入を受けたサーバに設けられた、不正侵入を行うための通信経路のこと
ウ　偽の送信元 IP アドレスをもったパケットを送ること
エ　本人に気付かれないように、利用者の操作や個人情報などを収集すること

［問28］マルウェアの活動傾向などを把握するための観測用センサが配備されるダークネットはどれか。

ア　インターネット上で到達可能、かつ、未使用の IP アドレス空間
イ　組織に割り当てられている IP アドレスのうち、コンピュータで使用されている IP アドレス空間
ウ　通信事業者が他の通信事業者などに貸し出す光ファイバ設備
エ　マルウェアに狙われた制御システムのネットワーク

［問29］IPsec に関する記述のうち、適切なものはどれか。

ア　IKE は IPsec の鍵交換のためのプロトコルであり、ポート番号 80 が使用される。
イ　暗号化アルゴリズムとして、HMAC-SHA1 が使用される。
ウ　トンネルモードを使用すると、エンドツーエンドの通信で用いるIPのヘッダまで含めて暗号化される。
エ　ホスト A とホスト B との間で IPsec による通信を行う場合、認証や暗号化アルゴリズムを両者で決めるために ESP ヘッダでなく AH ヘッダを使用する。

［問30］ICMP Flood 攻撃に該当するものはどれか。

ア　HTTP GET コマンド繰り返しを送ることによって、攻撃対象のサーバにコンテンツ送信の負荷を掛ける。
イ　ping コマンドを用いて大量の要求パケットを発信することによって、攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する。
ウ　コネクション開始要求に当たる SYN パケットを大量に送ることによって、攻撃対象のサーバに、接続要求ごとに応答を返すための過大な負荷を掛ける。
エ　大量の TCP コネクションを確立することによって、攻撃対象のサーバに接続を維持させ続けてリソースを枯渇させる。

［問31］RLO を利用した手口の説明はどれか。

ア　「コンピュータウイルスに感染している」といった偽の警告を出して利用者を脅し、ウイルス対策ソフトの購入などを迫る。
イ　脆弱性があるホストやシステムをあえて公開し、攻撃の内容を観察する。
ウ　ネットワーク機器の MIB 情報のうち監視項目の値の変化を感知し、セキュリティに関するイベントを SNMP マネージャに通知するように動作させる。
エ　文字の表示順を変える制御文字を利用し、ファイル名の拡張子を偽装する。

［問32］情報セキュリティにおけるクラッキングの説明として、適切なものはどれか。

ア　PC などの機器に対して、外部からの衝撃や圧力、落下、振動などの耐久テストを行う。
イ　悪意をもってコンピュータに不正侵入し、データを盗み見や破壊などを行う。
ウ　システム管理者として、ファイアウォールの設定など、情報機器の設定やメンテナンスを行う。
エ　組織のセキュリティ対策が有効に働いていることを確認するために監査を行う。

［問33］ポリモーフィック型ウイルスの説明として、適切なものはどれか。

ア　インターネットを介して、攻撃者が PC を遠隔操作する。
イ　感染するごとにウイルスのコードを異なる鍵で暗号化し、同一のパターンで検知されないようにする。
ウ　複数の OS で利用できるプログラム言語でウイルスを作成することによって、複数の OS 上でウイルスが動作する。
エ　ルートキットを利用してウイルスに感染していないように見せかけることによって、ウイルスを隠蔽する。

［問34］コンピュータウイルスに関する次の記述中の a、b に入れる字句の適切な組合せはどれか。

OS やアプリケーションの〔 a 〕を突くようなウイルスの感染予防には、ウイルス定義ファイルを最新の状態に保つことや〔 b 〕が必要である。

ア　a:脅威　　b:OS やアプリケーションにセキュリティパッチをあてること
イ　a:脅威　　b:ハードディスクの暗号化
ウ　a:脆弱性　b:OS やアプリケーションにセキュリティパッチをあてること
エ　a:脆弱性　b:ハードディスクの暗号化

［問35］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どれか。

ア　RFID
イ　rootkit
ウ　TKIP
エ　web beacon

［問36］ディジタルフォレンジクスの説明として、適切なものはどれか。

ア　あらかじめ設定した運用基準に従って、メールサーバを通過する送受信メールをフィルタリングすること
イ　磁気ディスクなどの書換え可能な記憶媒体を単に初期化するだけではデータを復元される可能性があるので、覆い隠すように上書きすること
ウ　不正アクセスなどコンピュータに関する犯罪の法的な証拠性を確保できるように、原因究明に必要な情報を保全、収集して分析すること
エ　ホストに対する外部からの攻撃や不正なアクセスを防御すること

［問37］通信プロトコルに関する記述のうち、適切なものはどれか。

ア　アナログ通信で用いられる通信プロトコルはない。
イ　国際機関が制定したものだけであり、メーカが独自に定めたものは通信プロトコルとは呼ばない。
ウ　通信プロトコルは正常時の動作手順だけが定義されている。
エ　メーカや OS が異なる機器同士でも、同じ通信プロトコルを使えば互いに通信することができる。

［問38］DNSSEC で実現できることはどれか。

ア　DNS キャッシュサーバからの応答中のリソースレコードが、権威 DNS サーバで管理されているものであり、改ざんされていないことの検証
イ　権威 DNS サーバと DNS キャッシュサーバとの通信を暗号化することによる、ゾーン情報の漏えいの防止
ウ　長音「ー」と漢数字「一」などの似た文字をドメイン名に用いて、正規サイトのように見せかける攻撃の防止
エ　利用者の URL の打ち間違いを悪用して、偽サイトに誘導する攻撃の検知

［問39］2 系統の装置から成るシステム構成方式 a～c に関して、片方の系に故障が発生したときのサービス停止時間が短い順に左から並べたものはどれか。

a デュアルシステム
b デュプレックスシステム(コールドスタンバイ方式)
c デュプレックスシステム(ホットスタンバイ方式)

ア a の片系装置故障　c の現用系装置故障　b の現用系装置故障
イ b の現用系装置故障　a の片系装置故障　c の現用系装置故障
ウ c の現用系装置故障　a の片系装置故障　b の現用系装置故障
エ c の現用系装置故障　b の現用系装置故障　a の片系装置故障

［問40］JIS Q 27002 における情報資産に対する脅威の説明はどれか。

ア 情報資産に害をもたらすおそれのある事象の原因
イ 情報資産に内在して、リスクを顕在化させる弱点
ウ リスク対策に費用をかけないでリスクを許容する選択
エ リスク対策を適用しても解消しきれず残存するリスク

［問41］A 社は顧客管理システムの開発を、情報システム子会社である B 社に委託し、B 社は要件定義を行った上で、設計・プログラミング・テストまでを協力会社である C 社に委託した。C 社では D 社員にその作業を担当させた。このとき、開発したプログラムの著作権はどこに帰属するか。ここで、関係者の間には、著作権の帰属に関する特段の取決めはないものとする。

ア A 社
イ B 社
ウ C 社
エ D 社員

［問42］サイバーセキュリティ基本法において、サイバーセキュリティの対象として規定されている情報の説明はどれか。

ア　外交、国家安全に関する機密情報に限られる。
イ　公共機関で処理される対象の手書きの書類に限られる。
ウ　個人の属性を含むプライバシー情報に限られる。
エ　電磁的方式によって、記録、発信、伝送、受信される情報に限られる。

［問43］特段の措置をとらずになされた個人情報取扱事業者の行為のうち、個人情報保護法に照らして適法な行為はどれか。

ア　開催したセミナで回収した、商品企画立案を目的としたアンケートに記載された参加者の氏名及び住所を、自社の販売促進セミナ案内用ダイレクトメール発送先住所録に登録した。
イ　開設しているWebサイトの問合せページで自社製品販売促進ダイレクトメール送付可否欄に可と記入した依頼者の氏名及び住所を、自社の製品販売促進用ダイレクトメール発送先住所録に登録した。
ウ　自社が主催した市場動向に関する勉強会の参加者リストの内容を、自社の子会社の製品販売促進用メールマガジン発送先アドレスリストに登録した。
エ　従業員が参加した同窓会で配布された同窓生名簿に記載されている、同窓生の氏名及び電話番号を、自社製品販売促進用コールセンタのアウトバウンド用電話番号リストに登録した。

［問44］個人情報保護法において、匿名加工情報として規定されている情報の説明はどれか。

ア　本人に対する不当な差別または偏見が生じないように人種・信条・病歴等が含まれる個人情報
イ　特定の個人を識別できないように加工した個人情報
ウ　本人の同意を得てデータベース等の事業に供している個人情報
エ　生存する個人に関する情報で、氏名・生年月日その他の記述によって特定の個人を識別できる情報

[問45] マイナンバー法(行政手続における特定の個人を識別するための番号の利用等に関する法律)に照らして適切なものはどれか。

ア　個人番号と法人番号の付番が規定されている。
イ　通知カードを紛失したときは、直ちに、その旨を総務省に届け出なければならない。
ウ　個人番号とすべき番号は、通知カードの申請時に生成される。
エ　個人番号カードには氏名、住所、生年月日、個人番号その他政令で定める事項などが記載されるが、性別は記載されない。

[問46] 刑法における、いわゆるコンピュータウイルスに関する罪となるものはどれか。

ア　ウイルス対策ソフトの開発、試験のために、新しいウイルスを作成した。
イ　自分に送られてきたウイルスに感染した電子メールを、それとは知らずに他者に転送した。
ウ　自分に送られてきたウイルスを発見し、ウイルスであることを明示してウイルス対策組織へ提供した。
エ　他人が作成したウイルスを発見し、後日これを第三者のコンピュータで動作させる目的で保管した。

[問47] 2011 年に経済産業省が公表した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」が策定された目的について述べたものはどれか。

ア　JIS Q 27002 の管理策を補完し、クラウドサービス利用者が情報セキュリティ対策を円滑に行えるようにする。
イ　クラウドサービス提供事業者に対して情報セキュリティ監査を実施する方法を利用者に提示する。
ウ　クラウドサービスの利用がもたらすセキュリティリスクをサービス提供事業者の視点で提示する。
エ　セキュリティリスクの懸念の少ないクラウドサービス提供事業者を利用者が選択できるような格付け基準を提供する。

［問48］下請代金支払遅延等防止法において、下請業者から受領したプログラムの返品を禁止しているのは、どの場合か。

ア　委託内容の一部を受領したが、下請業者の要員不足が原因で開発が遅れている旨の説明を受けた。
イ　親事業者と顧客との間の委託内容が変更になり、既に受領していたプログラムが不要になった。
ウ　開発途上で発生した仕様変更の内容、対価などを下請業者と合意していたが、受領したプログラムには仕様変更が反映されていなかった。
エ　受領時の通常のテストでは発見できなかった重大なバグが、受領後 5 か月経過した時点で発見された。

［問49］プロジェクト管理においてパフォーマンス測定に使用する EVM の管理対象の組みはどれか。

ア　コスト、スケジュール
イ　コスト、リスク
ウ　スケジュール、品質
エ　品質、リスク

［問50］IT サービスマネジメントにおける問題管理プロセスにおいて実施することはどれか。

ア　インシデントの発生後に暫定的にサービスを復旧させ、業務を継続できるようにする。
イ　インシデントの発生後に未知の根本原因を特定し、恒久的な解決策を策定する。
ウ　インシデントの発生に備えて、復旧のための設計をする。
エ　インシデントの発生を記録し、関係する部署に状況を連絡する。

以上

情報セキュリティマネジメント試験対策

模擬試験・予想問題

午前問題（50 問）

解答・解説編

［問1］エ
可用性とは、ユーザが使いたいときに使える、利用可能であるという意味です。生体認証や暗号化は「機密性」、改竄防止ができるディジタル署名は「完全性」への対応です。

［問2］ウ
「物理的」とは、「モノとして」という意味です。従業員は「人的」、ディジタル署名の付与やパスワードの定期的な変更などは「技術的」なセキュリティ対策に該当します。

［問3］ウ
耐タンパ性（Tamper Resistant）とは「見破られることの難しさ、解析することが困難な度合い」という意味です。この問題では、保存情報が守られる強さという意味です。

［問4］ウ
ISMS（Information Security Management System）を構築する組織は、保護すべき情報資産を特定し、リスク対策を決めなければなりません。

［問5］ア
情報セキュリティ方針は、組織のトップマネジメントが確立して、組織の全員に周知し、外部の関係者にも公表するものです。

［問6］ア
社員に対する情報セキュリティ教育は、全員に実施するのが適切です。「情報システム部門に所属する社員に限定する」のは誤りです。

［問7］ア
リスクファイナンスは、リスクが起こった場合に掛かる費用などの資金をあらかじめ確保する対策です。

［問8］ア
PDCA（Plan、Do、Check、Act）サイクルは、計画→実行（実施）→評価→改善（是正）の順序で行われます。

［問9］ウ

CSIRT（Computer Security Incident Response Team）は、コンピュータセキュリティインシデントに関する報告を受け取り、調査し、対応活動を行う組織の総称です。

［問10］イ
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したり記録したりする機能を持つ監視機器です。盗聴などに悪用されないように注意する必要があります。

［問11］ア
ESSID（Extended Service Set IDentifier）はネットワークの名前のようなものです。ESSID をステルス化（外部から見えなく）すると、不正アクセスの防止効果があります。

［問12］ウ
ESSID は管理者が変更できるので a は誤り。無線 LAN と電子レンジは電波干渉の可能性があり、端末をモデムとして利用するテザリングは無線でも行うので、b と c は正しい記述です。

［問13］エ
MDM は携帯端末を一元管理する仕組みです。BYOD は社員が自己所有する機器を業務で使うこと、ECM は社内の文書などのコンテンツを一元管理する仕組みです。

［問14］ウ
スマートフォンにパスワードによる画面のロック機能を設定することで、不正な利用を防ぎ、安全性を高めることができます。

［問15］ア
NIDS（Network Intrusion Detection System）はネットワーク型侵入検知システムのことで、ネットワーク内への不正侵入の試みを検知し、管理者に通知する機能があります。

［問16］エ
ベイジアン（Bayesian）フィルタリングは、利用者が振り分けた迷惑メールから特徴を学習して判定を行う学習型のスパムフィルターです。

［問17］イ
バイオメトリクス（生体）認証は、身体的な特徴で個人を識別するので、ID や鍵などを携帯する必要がないので紛失の心配もありません。

［問18］イ
SQL インジェクション攻撃は、データベースを操作する命令（SQL）で使われる特定の文字を、悪意を持って利用して、データベースに不正な実行をさせようとする攻撃です。

［問19］イ
WAF（Web Application Firewall）は、クライアントと Web サーバの間において、クライアントが Web サーバに送信されたデータを検査して、不正なデータを遮断する仕組みです。

［問20］エ
ワンタイムパスワードは「使い捨て」のパスワードのことで、1 回しか使えないので盗まれても使えないので「なりすまし」防止に効果が期待できます。

［問21］ウ
IDS（Intrusion Detection System）は、パケットを監視する侵入検知システム。ホスト型 IDS は、パターンマッチングを失敗させようとするタイプの攻撃でも検知できます。

［問22］イ
ファイルの複製をとっておき、後で内容まで照合すると、ファイルのあるレコードが変更されたときに、変更された内容も特定することができます。

［問23］ウ
CRYPTREC は、安全性を評価・監視し、暗号技術の適切な実装や運用を調査・検討するプロジェクト。「電子政府推奨暗号リスト」は、当該技術を推奨するリストです。

［問24］ウ
共通鍵暗号方式は暗号化と復号の鍵が同じで、公開鍵暗号方式に比べて仕組みがシンプルなため、処理時間は短くなります。

［問25］ウ
PKI（Public Key Infrastructure）は、電子証明書を「公開鍵」に対して発行することで正当性を証明する公開鍵基盤です。

［問26］エ
SPF（Sender Policy Framework）は、送信元の DNS サーバの SPF レコードにメール送信者のドメインが登録されているかどうかを確認する仕組みです。

［問27］ウ
IP スプーフィング（Spoofing、なりすまし）とは、偽の送信元 IP アドレスをもったパケットを送ることです。

［問28］ア
ダークネットは、インターネット上で到達可能、かつ、未使用の IP アドレス空間です。ライブネットは、割り当てられている IP アドレスのうち使用中の IP アドレス空間です。

［問29］ウ
IPsec は IP のセキュリティを強化したプロトコルです。トンネルモードを使用すると IP のヘッダまで含めて暗号化されます。IKE（Internet Key Exchange）は UDP ポート番号 500 で通信する IPsec 標準の鍵交換プロトコル。

［問30］イ
ICMP（Internet Control Message Protocol）Flood 攻撃は、ping コマンドを用いて大量の接続要求パケットを発信することによって、攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する攻撃手法。接続開始要求を大量に送る手法は SYN Flood 攻撃、大量の TCP コネクションを確立する手法は Connection Flood 攻撃です。

［問31］エ
RLO（Right to Left Override）は、文字を右から左へ向かって読むように表示順を変える制御文字のことです。悪用するとファイル名の拡張子の偽装などが可能になります。

［問32］イ
クラッキング（Cracking）は、悪意をもってコンピュータに不正侵入して、データを盗み見たり、破壊したりする行為です。

［問33］イ

ポリモーフィック型（Polymorphic、多形型の）ウイルスは、感染ごとにコードを異なる鍵で暗号化することで、パターン検知をすり抜けようとするタイプのウイルスです。

［問34］ウ
OS やアプリケーションの「脆弱性」を突くようなウイルスの感染予防には、ウイルス定義ファイルを最新の状態に保つことや「セキュリティパッチをあてること」が必要です。

［問35］イ
rootkit（ルートキット）は、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のパッケージの俗称です。

［問36］ウ
ディジタルフォレンジックスは、犯罪の原因究明に必要な情報を保全、収集して分析することです。Forensics は「科学捜査の」という意味です。

［問37］エ
メーカや OS が異なる機器同士でも、同じ通信プロトコル（Protocol、通信規約・通信手順）を使えば互いに通信することができます。

［問38］ア
DNSSEC（DNS Security Extensions）は、DNS サーバが、ディジタル署名を付加して応答することで、応答レコードの正当性、改ざんの有無が検証可能になる方式です。

［問39］ア
デュアルシステムは同じ処理を常に 2 つのシステムで行うことです。デュプレックスシステムには、予備系を起動させておく「ホット」スタンバイ、予備系を必要に応じて起動する「コールド」スタンバイがあります。

［問40］ア
情報セキュリティ管理策の実践のためのガイドラインである「ISO／IEC 27002」の日本語版が「JIS Q 27002」です。脅威は情報資産に害をもたらすおそれのある事象の「原因」、脆弱性はリスクを顕在化させる「弱点」という定義です。

［問41］ウ
著作権の帰属に関する特段の取決めがない場合、開発した著作物の著作権は委託

先であり、開発を担当した「C 社」に帰属します。

［問42］エ
サイバーセキュリティ基本法の規定では、サイバーセキュリティの対象となるのは、電磁的方式によって、記録、発信、伝送、受信される情報に限られます。

［問43］イ
「自社製品販売促進ダイレクトメール送付可否欄に可と記入した依頼者」は、本人の同意があるので、自社の製品販売促進ダイレクトメールを発送することができます。

［問44］イ
個人情報保護法における「匿名加工情報」とは、「特定の個人を識別できないように加工した個人情報」のことです。「本人に対する不当な差別または偏見が生じないように人種・信条・病歴等が含まれる個人情報」は「要配慮個人情報」です。

［問45］ア
法人番号は、特定の法人その他の団体を識別するための番号として指定されます。通知カードを紛失したときは「住所地市町村長」への届出が必要です。

［問46］エ
正当な理由なく「第三者のコンピュータで動作させる目的でコンピュータウイルスを保管すること」は、不正指令電磁的記録に関する罪に該当します。

［問47］ア
「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」は、クラウドサービスの提供事業者ではなく、利用者自らが活用することを企図して策定されています。

［問48］イ
下請法は、親事業者の地位の濫用を防止し、下請事業者に対する不公平な取引を是正することを目的とした法律です。

［問49］ア
EVM（Earned Value Management）は、コストやスケジュールの価値（Value）を定量的に管理する手法や考え方のことです。Earn は「稼ぐ・儲ける」という意味です。

［問50］イ
問題管理プロセスでは、インシデントの発生後に未知の根本原因を特定し、恒久的な解決策を策定します。

以上