

付録

模擬問題

◆ 午前 問題

試験時間：1 時間 30 分

問題番号：問 1 ～ 問 50

選択方法：全問必須

◆ 午前 解答と解説

◆ 午後 問題

試験時間：1 時間 30 分

問題番号：問 1 ～ 問 3

選択方法：全問必須

◆ 午後 解答と解説

Q

午前 問題

問1 情報セキュリティにおける“完全性”を脅かす攻撃はどれか。

- ア Webページの改ざん
- イ システム内に保管されているデータの不正コピー
- ウ システムを過負荷状態にするDoS攻撃
- エ 通信内容の盗聴

(平成26年春 基本情報技術者試験 午前 問39)

問2 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に残存するリスク

(平成22年春 応用情報技術者試験 午前 問41)

問3 マルウェアの説明として、適切なものはどれか。

- ア インターネットから社内ネットワークへの不正侵入を検知する仕組み
- イ コンピュータウイルス、ワームなどを含む悪意のあるソフトウェアの総称
- ウ ネットワークを介し、コンピュータ間でファイル共有を行うソフトウェア
- エ 話術や盗み聞きなどによって、社内の情報を盗み出す行為

(平成25年秋 ITパスポート試験 午前 問77)

問4 SQLインジェクション攻撃の説明はどれか。

- ア Webアプリケーションに問題があるとき、悪意のある問合せや操作を行う命令文を入力して、データベースのデータを不正に取得したり改ざんしたりする攻撃
- イ 悪意のあるスクリプトを埋め込んだWebページを訪問者に閲覧させて、別のWebサイトで、その訪問者が意図しない操作を行わせる攻撃
- ウ 市販されているDBMSの脆弱性を利用することによって、宿主となるデータベースサーバを探して自己伝染を繰り返し、インターネットのトラフィックを急増させる攻撃
- エ 訪問者の入力データをそのまま画面に表示するWebサイトに対して、悪意のあるスクリプトを埋め込んだ入力データを送ることによって、訪問者のブラウザで実行させる攻撃

(平成27年春 基本情報技術者試験 午前 問42)

問5 ソーシャルエンジニアリング手法を利用した標的型攻撃メールの特徴はどれか。

- ア 件名に“未承諾広告※”と記述されている。
- イ 件名や本文に、受信者の業務に関係がありそうな内容が記述されている。
- ウ 支払う必要がない料金を振り込ませるために、債権回収会社などを装い無差別に送信される。
- エ 偽のホームページにアクセスさせるために、金融機関などを装い無差別に送信される。

(平成25年春 応用情報技術者試験 午前 問40)

問6 企業内ネットワークやサーバに侵入するために攻撃者が組み込むものはどれか。

- | | |
|------------------|---------------|
| ア シンクライアントエージェント | イ ストリクトルーティング |
| ウ デジタルフォレンジックス | エ バックドア |

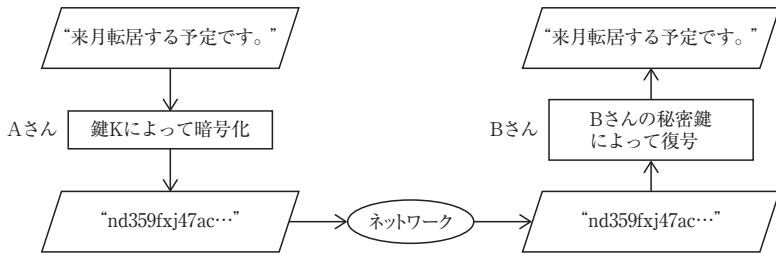
(平成26年春 基本情報技術者試験 午前 問43)

問7 データベースで管理されるデータの暗号化に用いることができ、かつ、暗号化と復号とで同じ鍵を使用する暗号化方式はどれか。

- | | | | |
|-------|-------|-------|-----------|
| ア AES | イ PKI | ウ RSA | エ SHA-256 |
|-------|-------|-------|-----------|

(平成27年春 基本情報技術者試験 午前 問39)

問8 公開鍵暗号方式を用いて、図のようにAさんからBさんへ、他人に秘密にしておきたい文章を送るとき、暗号化に用いる鍵Kとして、適切なものはどれか。



ア Aさんの公開鍵 イ Aさんの秘密鍵 ウ Bさんの公開鍵 エ 共通の秘密鍵

(平成27年春 基本情報技術者試験 午前 問40)

問9 デジタル署名における署名鍵の用い方と、デジタル署名を行う目的のうち、適切なものはどれか。

- ア 受信者が署名鍵を使って、暗号文を元のメッセージに戻すことができるようにする。
- イ 送信者が固定文字列を付加したメッセージを署名鍵を使って暗号化することによって、受信者がメッセージの改ざん部位を特定できるようにする。
- ウ 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する。
- エ 送信者が署名鍵を使ってメッセージを暗号化することによって、メッセージの内容を関係者以外に分からないようにする。

(平成27年春 基本情報技術者試験 午前 問38)

問10 バイオメトリクス認証には、身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

- ア 血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。
- イ 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。
- ウ 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抽出して認証する。
- エ 隆線によって形作られる紋様からマニキュシャと呼ばれる特徴点を抽出して認証する。

(平成27年春 基本情報技術者試験 午前 問41)

問11 デジタル証明書をもつA氏が、B商店に対して電子メールを使って商品の注文を行うときに、A氏は自分の秘密鍵を用いてデジタル署名を行い、B商店はA氏の公開鍵を用いて署名を確認する。この手法によって実現できることはどれか。ここで、A氏の秘密鍵はA氏だけが使用できるものとする。

- ア A氏からB商店に送られた注文の内容は、第三者に漏れないようにできる。
- イ A氏から発信された注文は、B商店に届くようにできる。
- ウ B商店に届いた注文は、A氏からの注文であることを確認できる。
- エ B商店は、A氏に商品を売ることが許可されていることを確認できる。

(平成26年秋 基本情報技術者試験 午前 問37)

問12 特定の認証局が発行したCRL (Certificate Revocation List)に関する説明のうち、適切なものはどれか。

- ア CRLには、失効したデジタル証明書に対応する秘密鍵が登録される。
- イ CRLには、有効期限内のデジタル証明書のうち破棄されているデジタル証明書と破棄された日時に対応が提示される。
- ウ CRLは、鍵の漏えい、破棄申請の状況をリアルタイムに反映するプロトコルである。
- エ 有効期限切れで失効したデジタル証明書は、所有者が新たなデジタル証明書を取得するまでの間、CRLに登録される。

(平成26年春 情報セキュリティスペシャリスト試験 午前Ⅱ 問1)

問13 ISMSにおいて定義することが求められている情報セキュリティ基本方針に関する記述のうち、適切なものはどれか。

- ア 重要な基本方針を定めた機密文書であり、社内の関係者以外の目に触れないようにする。
- イ 情報セキュリティの基本方針を述べたものであり、ビジネス環境や技術が変化しても変更してはならない。
- ウ 情報セキュリティのための経営陣の方向性及び支持を規定する。
- エ 特定のシステムについてリスク分析を行い、そのセキュリティ対策とシステム運用の詳細を記述する。

(平成25年秋 応用情報技術者試験 午前 問40)

問14 組織の活動に関する記述a～dのうち、ISMSの特徴として、適切なものを全て挙げたものはどれか。

- a 一過性の活動で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。
- d 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

(平成27年春 ITパスポート試験 午前 問81)

問15 システム障害を想定した事業継続計画(BCP)を策定する場合、ビジネスインパクト分析での実施事項はどれか。

- ア BCPの有効性を検証するためのテストを実施する。
- イ 情報システム障害時の代替手順と復旧手順について関係者を集めて教育する。
- ウ 情報システムに関する内外の環境の変化を踏まえてBCPの内容を見直す。
- エ 情報システムに許容される最大停止時間を決定する。

(平成24年春 基本情報技術者試験 午前 問42)

問16 リスクアセスメントに関する記述のうち、適切なものはどれか。

- ア 以前に洗い出された全てのリスクへの対応が完了する前に、リスクアセスメントを実施することは避ける。
- イ 将来の損失を防ぐことがリスクアセスメントの目的なので、過去のリスクアセスメントで利用されたデータを参照することは避ける。
- ウ 損失額と発生確率の予測に基づくリスクの大きさに従うなどの方法で、対応の優先順位を付ける。
- エ リスクアセスメントはリスクが顕在化してから実施し、損失額に応じて対応の予算を決定する。

(平成26年秋 基本情報技術者試験 午前 問39)

問17 リスク共有(リスク移転)に該当するものはどれか。

- ア 損失の発生率を低下させること
- イ 保険への加入などで、他者との間でリスクを分散すること
- ウ リスクの原因を除去すること
- エ リスクを扱いやすい単位に分解するか集約すること

(平成25年秋 基本情報技術者試験 午前 問39)

問18 JPCERT/CCの説明はどれか。

- ア 工業標準化法に基づいて経済産業省に設置されている審議会であり、工業標準化全般に関する調査・審議を行っている。
- イ 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり、総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される。
- ウ 特定の政府機関や企業から独立した組織であり、国内のコンピュータセキュリティインシデントに関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止策の検討や助言を行っている。
- エ 内閣官房に設置され、我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である。

(平成27年春 応用情報技術者試験 午前 問40)

問19 基本評価基準、現状評価基準、環境評価基準の三つの基準でIT製品のセキュリティ脆弱性の深刻さを評価するものはどれか。

- ア CVSS
- イ ISMS
- ウ PCI DSS
- エ PMS

(平成26年秋 情報セキュリティスペシャリスト試験 午前Ⅱ 問7)

問20 複数の業務システムがある場合のアクセス管理の方法のうち、最も適切なものはどれか。

- ア 業務の担当変更に対応するために、業務グループごとに共通の利用者IDを使用する。
- イ 人事異動が頻繁に発生する場合には、年初にまとめてアクセス権限の変更を行う。
- ウ 新入社員の名簿に基づいて、あらかじめ全業務システムに全員の利用者登録を実施しておく。
- エ 利用者の職位にかかわらず、業務システムごとに役割に応じて適切なアクセス権限の設定を行う。

(平成24年春 基本情報技術者試験 午前 問56)

問21 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 対象は、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。

(平成27年春 ITパスポート試験 午前 問63)

問22 WAF (Web Application Firewall) を利用する目的はどれか。

- ア Webサーバ及びWebアプリケーションに起因する脆弱性^{弱い}への攻撃を遮断する。
- イ Webサーバ内でワームの侵入を検知し、ワームの自動駆除を行う。
- ウ Webサーバのコンテンツ開発の結合テスト時にWebアプリケーションの脆弱性や不整合を検知する。
- エ Webサーバのセキュリティホールを発見し、OSのセキュリティパッチを適用する。

(平成26年秋 基本情報技術者試験 午前 問41)

問23 通信を要求したPCに対し、ARPの仕組みを利用して実現できる通信可否の判定方法のうち、最も適切なものはどれか。

- ア PCにインストールされているソフトウェアを確認し、登録されているソフトウェアだけがインストールされている場合に通信を許可する。
- イ PCのMACアドレスを確認し、事前に登録されているMACアドレスである場合だけ通信を許可する。
- ウ PCのOSのパッチ適用状況を確認し、最新のパッチが適用されている場合だけ通信を許可する。
- エ PCのマルウェア対策ソフトの定義ファイルを確認し、最新になっている場合だけ通信を許可する。

(平成24年春 基本情報技術者試験 午前 問44)

問24 クライアントPCで行うマルウェア対策のうち、適切なものはどれか。

- ア PCにおけるウイルスの定期的な手動検査では、ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
- イ ウイルスがPCの脆弱性を突いて感染しないように、OS及びアプリケーションの修正パッチを適切に適用する。
- ウ 電子メールに添付されたウイルスに感染しないように、使用しないTCPポート宛での通信を禁止する。
- エ ワームが侵入しないように、クライアントPCに動的グローバルIPアドレスを付与する。

(平成25年秋 基本情報技術者試験 午前 問42)

問25 ウイルス対策ソフトのパターンマッチング方式を説明したものはどれか。

- ア 感染前のファイルと感染後のファイルを比較し、ファイルに変更が加わったかどうかを調べてウイルスを検出する。
- イ 既知ウイルスのシグネチャと比較して、ウイルスを検出する。
- ウ システム内でのウイルスに起因する異常現象を監視することによって、ウイルスを検出する。
- エ ファイルのチェックサムと照合して、ウイルスを検出する。

(平成26年秋 基本情報技術者試験 午前 問42)

問26 電子メール送信時に送信者に対して宛先アドレスの確認を求めるのが有効であるセキュリティ対策はどれか。

- ア OP25Bによるスパム対策
- イ SPFによるスパム対策
- ウ 電子メールの誤送信対策
- エ 電子メールの不正中継対策

(平成23年秋 基本情報技術者試験 午前 問44)

問27 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。

(平成21年秋 情報セキュリティスペシャリスト試験 午前Ⅱ 問6)

問28 機密ファイルが格納されていて、正常に動作するPCの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策のうち、適切なものはどれか。

- ア 異なる圧縮方式で、機密ファイルを複数回圧縮する。
- イ 専用の消去ツールで、磁気ディスクのマスタブートレコードを複数回消去する。
- ウ 特定のビット列で、磁気ディスクの全領域を複数回上書きする。
- エ ランダムな文字列で、機密ファイルのファイル名を複数回変更する。

(平成25年春 基本情報技術者試験 午前 問41)

問29 HTTPS (HTTP over SSL/TLS) の機能を用いて実現できるものはどれか。

- ア SQLインジェクションによるWebサーバへの攻撃を防ぐ。
- イ TCPポート80番と443番以外の通信を遮断する。
- ウ Webサーバとブラウザの間の通信を暗号化する。
- エ Webサーバへの不正なアクセスをネットワーク層でのパケットフィルタリングによって制限する。

(平成26年秋 基本情報技術者試験 午前 問43)

問30 Webサーバを使ったシステムにおいて、インターネットから受け取ったリクエストをWebサーバに中継する仕組みはどれか。

- | | |
|-----------|-------------|
| ア DMZ | イ フォワードプロキシ |
| ウ プロキシARP | エ リバースプロキシ |

(平成21年秋 情報セキュリティスペシャリスト試験 午前Ⅱ 問21)

問31 不正アクセス禁止法において、不正アクセス行為に該当するものはどれか。

- ア 会社の重要情報にアクセスし得る者が株式発行の決定を知り、情報の公表前に当該会社の株を売買した。
- イ コンピュータウイルスを作成し、他人のコンピュータの画面表示をでたらめにする被害をもたらした。
- ウ 自分自身で管理運営するホームページに、昨日の新聞に載った報道写真を新聞社に無断で掲載した。
- エ 他人の利用者ID、パスワードを許可なく利用して、アクセス制御機能によって制限されているWebサイトにアクセスした。

(平成23年特別 基本情報技術者試験 午前 問80)

問32 個人情報に関する記述のうち、個人情報保護法に照らして適切なものはどれか。

- ア 構成する文字列やドメイン名によって特定の個人を識別できるメールアドレスは、個人情報である。
- イ 個人に対する業績評価は、その個人を識別できる情報が含まれていても、個人情報ではない。
- ウ 新聞やインターネットなどで既に公表されている個人の氏名、性別及び生年月日は、個人情報ではない。
- エ 法人の本店住所、支店名、従業員数及び代表電話番号は、個人情報である。

(平成25年秋 基本情報技術者試験 午前 問80)

問33 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。

(平成27年春 基本情報技術者試験 午前 問79)

問34 電子署名法に関する記述のうち、適切なものはどれか。

- ア 電子署名技術は共通鍵暗号技術によるものと規定されている。
- イ 電子署名には、電磁的記録以外の、コンピュータ処理の対象とならないものも含まれる。
- ウ 電子署名には、民事訴訟法における押印と同様の効力が認められている。
- エ 電子署名の認証業務を行うことができるのは、政府が運営する認証局に限られる。

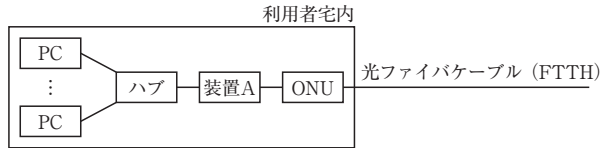
(平成27年春 応用情報技術者試験 午前 問80)

問35 不正競争防止法によって保護される対象として規定されているものはどれか。

- ア 自然法則を利用した技術的思想の創作のうち高度なものであって、プログラム等を含む物と物を生産する方法
- イ 著作物を翻訳し、編曲し、若しくは変形し、又は脚色し、映画化し、その他翻案することにより創作した著作物
- ウ 秘密として管理されている事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの
- エ 法人等の発意に基づきその法人等の業務に従事する者が職務上作成するプログラム著作物

(平成25年春 基本情報技術者試験 午前 問78)

問36 LANに接続されている複数のPCを、FTTHを使ってインターネットに接続するシステムがあり、装置AのWAN側インタフェースには1個のグローバルIPアドレスが割り当てられている。この1個のグローバルIPアドレスを使って複数のPCがインターネットを利用するのに必要となる装置Aの機能はどれか。



ア DHCP
ウ PPPoE

イ NAPT (IPマスカレード)
エ パケットフィルタリング

(平成25年春 基本情報技術者試験 午前 問34)

問37 IPv4で192.168.30.32/28のネットワークに接続可能なホストの最大数はどれか。

ア 14

イ 16

ウ 28

エ 30

(平成26年春 基本情報技術者試験 午前 問35)

問38 “中間テスト”表からクラスごと、教科ごとの平均点を求め、クラス名、教科名の昇順に表示するSQL文中のaに入れるべき字句はどれか。

中間テスト(クラス名, 教科名, 学生番号, 名前, 点数)

〔SQL文〕

SELECT クラス名, 教科名, AVG(点数) AS 平均点

FROM 中間テスト

a

ア GROUP BY クラス名, 教科名 ORDER BY クラス名, AVG(点数)

イ GROUP BY クラス名, 教科名 ORDER BY クラス名, 教科名

ウ GROUP BY クラス名, 教科名, 学生番号 ORDER BY クラス名, 教科名, 平均点

エ GROUP BY クラス名, 平均点 ORDER BY クラス名, 教科名

(平成25年春 基本情報技術者試験 午前 問28)

問39 データベースの排他制御のロック獲得の可能性のうち、適切なものはどれか。

- ア あるトランザクションが共有ロックを獲得している資源に対して、別のトランザクションが共有ロックを獲得することは可能である。
- イ あるトランザクションが共有ロックを獲得している資源に対して、別のトランザクションが専有ロックを獲得することは可能である。
- ウ あるトランザクションが専有ロックを獲得している資源に対して、別のトランザクションが共有ロックを獲得することは可能である。
- エ あるトランザクションが専有ロックを獲得している資源に対して、別のトランザクションが専有ロックを獲得することは可能である。

(平成25年春 基本情報技術者試験 午前 問30)

問40 東京～大阪及び東京～名古屋がそれぞれ独立した通信回線で接続されている。東京～大阪の稼働率は0.9、東京～名古屋の稼働率は0.8である。東京～大阪の稼働率を0.95以上に改善するために、大阪～名古屋にバックアップ回線を新設することを計画している。新設される回線の稼働率は、最低限幾ら必要か。

- ア 0.167 イ 0.205 ウ 0.559 エ 0.625

(平成26年秋 基本情報技術者試験 午前 問14)

問41 ソフトウェア資産管理に対する監査のチェックポイントとして、最も適切なものはどれか。

- ア ソフトウェアの提供元の開発体制について考慮しているか。
- イ ソフトウェアの導入時に既存システムとの整合性を評価しているか。
- ウ ソフトウェアのライセンス証書などのエビデンスが保管されているか。
- エ データベースの分割などによって障害の局所化が図られているか。

(平成26年秋 基本情報技術者試験 午前 問60)

問42 ITサービスを廃止する際には、使われていた資産を包括的に識別し、余分な資産の除去や解放を適切に行うことが重要である。除去すべきでない資産を誤って除去することが原因で起こる可能性がある事象はどれか。

- ア 磁気ディスク内の使わなくなる領域の無駄使い
- イ ソフトウェアやハードウェアの保守料金の過払い
- ウ ソフトウェアライセンスの無駄使い
- エ 廃止するITサービスと資産を共有している別のITサービスでのインシデントの発生

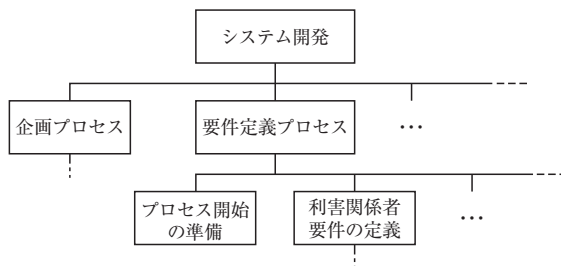
(平成26年秋 基本情報技術者試験 午前 問56)

問43 システムの運用に関する記述のうち、適切なものはどれか。

- ア 故障した構成品目を切り離し、システムのより重要な機能を存続させることを、縮退運転という。
- イ 障害時のファイルの回復を目的として、定期的にファイルを別の記憶媒体に保存することを、リストアという。
- ウ チェックポイントで記録しておいたデータを使用して、プログラムの実行を再開することを、リブートという。
- エ データベースを変更が行われた以前の状態に復元することを目的としたトランザクション処理の記録を、データログという。

(平成26年秋 基本情報技術者試験 午前 問57)

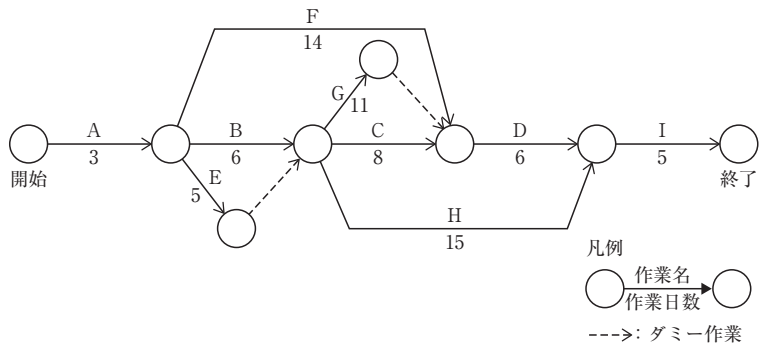
問44 図のように、プロジェクトチームが実行すべき作業を上位の階層から下位の階層へ段階的に分解したものを何と呼ぶか。



- ア CPM
- イ EVM
- ウ PERT
- エ WBS

(平成26年春 基本情報技術者試験 午前 問52)

問45 図は、あるプロジェクトの作業(A～I)とその作業日数を表している。このプロジェクトが終了するまでに必要な最短日数は何日か。



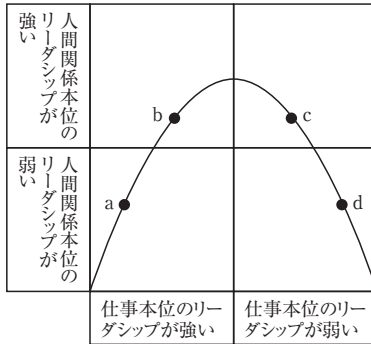
- ア 27 イ 28 ウ 29 エ 31

(平成27年春 基本情報技術者試験 午前 問54)

問46 リーダシップのスタイルは、その組織の状況に合わせる必要がある。組織とリーダーシップの関係に次のことが想定できるとすると、野球チームの監督のリーダーシップのスタイルとして、図のdと考えられるものはどれか。

〔組織とリーダーシップの関係〕

組織は発足当時、構成員や仕組みの成熟度が低いので、リーダーが仕事本位のリーダーシップで引っ張っていく。成熟度が上がるにつれ、リーダーと構成員の人間関係が培われ、仕事本位から人間関係本位のリーダーシップに移行していく。更に成熟度が進むと、構成員は自主的に行動でき、リーダーシップは仕事本位、人間関係本位のいずれもが弱まっていく。



- ア うるさく言うのも半分くらいで勝てるようになってきた。
- イ 勝つためには選手と十分に話し合って戦略を作ることだ。
- ウ 勝つためには選手に戦術の立案と実行を任せることだ。
- エ 選手をきちんと管理することが勝つための条件だ。

(平成25年秋 応用情報技術者試験 午前 問74)

問47 事業年度初日の平成21年4月1日に、事務所用のエアコンを100万円で購入した。平成23年3月31日現在の帳簿価額は何円か。ここで、耐用年数は6年、減価償却は定額法、定額法の償却率は0.167、残存価額は0円とする。

- ア 332,000
- イ 499,000
- ウ 666,000
- エ 833,000

(平成23年秋 基本情報技術者試験 午前 問76)

問48 エンタープライズアーキテクチャの“四つの分離体系”に含まれるアーキテクチャは、ビジネスアーキテクチャ、テクノロジーアーキテクチャ、アプリケーションアーキテクチャともう一つはどれか。

ア システムアーキテクチャ

イ ソフトウェアアーキテクチャ

ウ データアーキテクチャ

エ バスアーキテクチャ

(平成25年秋 基本情報技術者試験 午前 問62)

問49 共通フレームによれば、要件定義プロセスの活動内容には、利害関係者の識別、要件の識別、要件の評価、要件の合意などがある。このうち、要件の識別において実施する作業はどれか。

ア システムのライフサイクルの全期間を通して、どの工程でどの関係者が参画するのかを明確にする。

イ 抽出された要件を確認して、矛盾点や曖昧な点をなくし、一貫性がある要件の集合として整理する。

ウ 矛盾した要件、実現不可能な要件などの問題点に対する解決方法を利害関係者に説明し、合意を得る。

エ 利害関係者から要件を漏れなく引き出し、制約条件や運用シナリオなどを明らかにする。

(平成26年秋 基本情報技術者試験 午前 問66)

問50 CSR 調達に該当するものはどれか。

ア コストを最小化するために、最も安価な製品を選ぶ。

イ 災害時に調達が可能となる事態を避けるために、調達先を複数化する。

ウ 自然環境、人権などへの配慮を調達基準として示し、調達先に遵守を求める。

エ 物品の購買に当たってEDIを利用し、迅速・正確な調達を行う。

(平成26年秋 基本情報技術者試験 午前 問67)

A

午前 解答と解説

問1

《解答》ア

完全性とは、情報を書き換えられないようにすることです。具体例は、Webページが改ざんされないように、サーバへのアクセスを制限することなどが完全性の対策です。したがって、アが正解です。

イ、エ 機密性を脅かす脅威です。

ウ 可用性を脅かす攻撃です。

問2

《解答》ア

情報資産に対する脅威とは、システムや組織に損害を与える可能性があるインシデントの潜在的な原因です。したがって、アが正解です。

イ 脆弱性の説明です。

ウ リスク保有(リスク受容)の説明です。

エ 残留リスクの説明です。

問3

《解答》イ

マルウェアとは、悪意のあるソフトウェアの総称です。不正ソフトウェアとも呼ばれ、ウイルスやワームはマルウェアに含まれます。したがって、イが正解です。

ア IDS (Intrusion Detection System : 侵入検知システム)の説明です。

ウ ファイル共有ソフトの説明です。

エ ソーシャルエンジニアリングの説明です。

問4

《解答》ア

SQLインジェクションは、Webアプリケーションにおけるセキュリティ上の脅威のうち、データベースの問合せの際に制御記号などを混入させることで不正な動作を実行させるものです。したがって、アが正解です。

イ クロスサイトリクエストフォージェリ攻撃の説明です。

ウ DBMSに感染するマルウェアの攻撃の説明です。

エ クロスサイトスクリプティング攻撃の説明です。

問5

《解答》イ

ソーシャルエンジニアリング手法とは、技術ではなく、人間の心理や社会的な性質を利用した攻撃手法です。また、標的型攻撃メールとは、不特定多数向けではなく、ある特定の組織などにターゲットを絞った攻撃メールです。そのため、標的型攻撃メールでは、件名や本文に、ターゲットとなる受信者の業務に関係がありそうな内容が書かれています。したがって、イが正解です。

ア 広告メールの件名です。

- ウ 架空請求詐欺メールの説明です。
- エ フィッシングサイトに誘導するメールの説明です。

問6**《解答》エ**

攻撃者が正規の手続き(ログインなど)を行わずにシステムを利用できるように組み込む通信経路をバックドアといいます。したがって、エが正解です。

- ア シンクライアントとは、端末では基本的に処理を行わず、サーバ側でほとんどの処理を行う形態です。シンクライアントエージェントは、端末のソフトウェアで、サーバ側の処理を受け取るために存在します。
- イ ストリクトルーティングとは、IPネットワークのルーティングにおいて、送信元のルータが転送経路を全て決定する方式です。
- ウ デジタルフォレンジックスとは、不正アクセスや機密情報の漏えいなどで法的な紛争が生じた際に、原因究明や捜査に必要なデータを収集・分析し、その法的な証拠性を明らかにする手段や技術の総称です。

問7**《解答》ア**

暗号化と復号とで同じ鍵を使用する暗号化方式は、共通鍵暗号方式です。選択肢の中で共通鍵暗号方式は、AES (Advanced Encryption Standard)のみです。したがって、アが正解です。

- イ PKI (Public Key Infrastructure: 公開鍵基盤)は、公開鍵暗号方式を利用した社会基盤(インフラ)です。
- ウ 公開鍵暗号方式の一つです。開発者3名の頭文字から名付けられています。
- エ ハッシュアルゴリズムの一つです。

問8**《解答》ウ**

Aさんが鍵Kによって暗号化した文章は、Bさんによって復号できなければなりません。Bさんが復号に使用する「Bさんの秘密鍵」で復号できるのは、「Bさんの公開鍵」で暗号化された文章です。したがって、ウが正解です。

問9**《解答》ウ**

デジタル署名を行う目的は、送信者の確認と改ざんの検知です。送信者は、メッセージのハッシュ値に送信者の秘密鍵を使ってデジタル署名を作成します。受信者は、送信者の公開鍵でデジタル署名を復号し、メッセージのハッシュ値との一致を確認することで、送信者が正しいこと、改ざんが行われていないことを確認できます。したがって、ウが正解です。

- ア 受信者がデジタル署名を確認するのに必要なものは、送信者の公開鍵です。
- イ 改ざんの検知は可能ですが、改ざん部位を特定することはできません。
- エ メッセージの内容を関係者以外に分からないようにするためには、S/MIMEなどの暗号化の手法を使う必要があります。

問10

《解答》イ

バイオメトリクス認証の行動的特徴を抽出して認証する方式としては、サイン(筆跡)、キーストロークなどがあります。サインは記入時の速度や筆圧の特徴を利用し、キーストロークでは打鍵の速度やタイミングの特徴を利用します。したがって、イが正解です。

その他の選択肢は、身体的特徴を用いた方式です。

問11

《解答》ウ

秘密鍵はA氏しかもっていないため、A氏が自分の秘密鍵を用いてデジタル署名を行うことはA氏本人にしかできないことです。したがって、ウが正解です。

ア デジタル署名では、内容の暗号化は行いません。

イ、エ デジタル署名では確認できない内容です。

問12

《解答》イ

CRLは、失効したデジタル証明書のシリアル番号と、失効した日時を記したリストです。したがって、イが正解です。

ア CRLには、失効したデジタル証明書に対応する“シリアルナンバー”が登録されます。

ウ デジタル証明書の失効状態を取得するためのプロトコルは、OCSP (Online Certificate Status Protocol) です。

エ 有効期限切れとなった証明書はCRLには記載されません。

問13

《解答》ウ

情報セキュリティ基本方針は、情報セキュリティに対する組織の基本的な考え方や方針を示すもので、経営陣によって承認されます。目的や対象範囲、管理体制や罰則などについて記述されており、全従業員及び関係者に通知して公表されます。したがって、ウが正解です。

ア 公開文書であり、基本的に公開されます。

イ ビジネス環境や技術の変化によって変更していきます。

エ 情報セキュリティリスクアセスメントの説明です。

問14

《解答》イ

ISMS (情報セキュリティマネジメントシステム)は、組織の情報セキュリティを管理するための仕組みです。

a PDCAサイクルを繰り返し、管理・改善を行っていくので、適切です。

b トップマネジメントのリーダーシップが必須のトップダウン活動です。

c 経営の一環として全社で行うべきもので、経営に関わる企業のトップがリーダーシップをとり実現させていく必要があるため、適切です。

d プロジェクトの説明です。ISMSでは終了期限はありません。

したがって、該当するのはa、cなので、イが正解です。

問15

《解答》エ

IT サービス継続性管理では、災害のインパクトを定量化するためにビジネスインパクト分析 (BIA : Business Impact Analysis) を行います。BIA では、情報システムのビジネスへの影響を調査し、情報システムに許容される最大停止時間 (RTO : Recovery Time Objective) を決定します。したがって、エが正解です。

ア テストで実施する事項です。

イ 教育・訓練で実施する事項です。

ウ 監査で実施する事項です。

問16

《解答》ウ

リスクアセスメントとは、リスク特定、リスク分析、リスク評価を行うプロセス全体のことです。リスク分析では、リスクの発生確率を求め、実際にリスクが起こったときの影響の大きさを考えます。リスク評価では、リスクを評価し、優先度を付けていきます。したがって、ウが正解です。

ア リスクアセスメントにより、リスクを発見し、認識するので誤りです。

イ リスクアセスメントでは、過去のデータを参照することで効率化を行います。

エ リスクアセスメントはリスクが“顕在化する前に”実施します。

問17

《解答》イ

リスク共有 (リスク移転、リスク分散) は、リスクを第三者と分割することです。保険をかけるなどで、リスク発生時の費用負担を外部に分散させる方法があります。したがって、イが正解です。

ア リスク最適化 (リスク低減) に該当します。

ウ リスク回避に該当します。

エ リスク分解とリスク集約に該当します。

問18

《解答》ウ

JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) とは、日本国内のセキュリティインシデントに関する報告を受け付ける機関で、対応の支援、発生状況の把握などの様々な活動を行っています。したがって、ウが正解です。

ア 日本工業標準調査会 (JISC : Japanese Industrial Standards Committee) の説明です。

イ CRYPTREC (Cryptography Research and Evaluation Committees) の説明です。

エ 内閣サイバーセキュリティセンター (National center of Incident readiness and Strategy for Cybersecurity) の説明です。

問19

《解答》ア

基本評価基準 (Base Metrics)、現状評価基準 (Temporal Metrics)、環境評価基準 (Environmental Metrics) の三つの基準でIT製品のセキュリティ脆弱性の深刻さを評価するものは、CVSS (Common Vulnerability Scoring System : 共通脆弱性評価システム) です。したがって、アが正解です。

イ 情報セキュリティマネジメントシステム (Information Security Management System : ISMS) です。

- ウ PCIデータセキュリティスタンダード (Payment Card Industry Data Security Standard : PCI DSS) です。
- エ 個人情報保護マネジメントシステム (Personal Information Protection Management Systems : PMS) です。

問20**《解答》エ**

アクセス管理では、Need-to-know（最小権限）の原則で、必要最小限のアクセス権限を設定する必要があります。そのため、職位が高い人にすべての権限を与えることは適切ではなく、利用者の職務の範囲内でアクセス権限を与えることが大切です。したがって、エが正解です。

ア 担当者ごとに利用者IDを使用する必要があります。

イ 人事異動があった場合は、転出者のアクセス権限を不要になった時点で変更する必要があります。

ウ 新入社員のうち、業務システムの利用者のみ登録を行います。

問21**《解答》エ**

情報セキュリティ教育は、全ての人に同じ教育を行う必要はなく、社員の担当業務、役割及び責任に応じて内容を変えることは適切です。したがって、エが正解となります。

ア 再教育は定期的に行う必要があります。

イ 業務を開始する前に実施します。

ウ 情報資産にアクセスする社員以外にも関係者全員が対象になります。

問22**《解答》ア**

WAF (Web Application Firewall) は、Webアプリケーションの防御に特化したファイアウォールです。SQLインジェクションやクロスサイトスクリプティングなど、Webに特化した攻撃に対して、きめ細かくアクセス制御を行うことができます。したがって、アが正解です。

イ ウイルス対策ソフトを利用する目的です。

ウ Webアプリケーション脆弱性チェックツールを利用する目的です。

エ OSのアップデートを行う目的です。

問23**《解答》イ**

ARP (Address Resolution Protocol) とは、IPアドレスから、そのIPアドレスが設定されたホストのMACアドレスを取得するプロトコルです。IPアドレス、またはMACアドレスでフィルタリングすることで通信可否の判定を行うことができます。したがって、イが正解です。

その他の選択肢は、検疫ネットワークで利用される判定方法です。

問24**《解答》イ**

マルウェアとは、悪意のあるソフトウェアの総称です。マルウェア対策には、ウイルス対策ソフトをインストールすること、OS及びアプリケーションのアップデートを行って修正パッチを適切に適用することが有効です。したがって、イが正解です。

ア 作成日時を偽装している場合もあるので、全てのファイルを対象とします。

- ウ TCPポートの通信を禁止することと、添付ファイルがウイルスに感染することは関連がありません。
- エ グローバルIPアドレスで通信する場合、インターネットと直接通信が行われるため、ワームの侵入確率は上がります。

問25**《解答》イ**

ウイルス対策ソフトは、ウイルスをはじめとするマルウェアを検出するためのソフトウェアです。ウイルス定義ファイル(パターンファイル)と呼ばれるファイルと比較することでウイルスを検出するパターンマッチングと呼ばれる手法が主流です。したがって、イが正解です。

- ア、エ ファイルの改ざんを検出する方法です。
- ウ ビヘイビア法の説明です。

問26**《解答》ウ**

送信者が宛先アドレスを確認するのは、宛先アドレスを間違えて電子メールを誤送信してしまう可能性を防ぐためです。したがって、ウが正解です。

- ア OP25B (Outbound Port 25 Blocking)は、プロバイダのメールサーバを経由せずに直接、25番ポートで外部にSMTP通信を行うことを防止する対策です。
- イ SPF (Sender Policy Framework)は、差出人のIPアドレスなどを基にメールのドメインの正当性を検証する方法です。
- エ 不正中継は、関係のない第三者に、サーバなどを中継に利用されることです。

問27**《解答》ア**

IDS (Intrusion Detection System: 侵入検知システム)は、ネットワークやホストをリアルタイムで監視し、侵入や攻撃など不正なアクセスを検知したら管理者に通知するシステムです。IDSには、ネットワークに接続されてネットワーク全般を監視するNIDS (ネットワーク型IDS)があり、ネットワーク全体を監視できる、ホストに負担がかからないなどのメリットがあります。したがって、アが正解です。

- イ HIDS (ホスト型IDS)の特徴です。
- ウ ペネトレーションテストの説明です。
- エ リスクアセスメントの中でのリスク分析の説明です。

問28**《解答》ウ**

磁気ディスクを廃棄する場合は、情報漏えいを防ぐために、記録されているデータの読出しができないようにしてから廃棄する必要があります。磁気ディスク装置本体を物理的に破壊する、記録領域全体を特定のビット列で複数回上書きし、記録されていたデータを読み出せないようにするなどの対処方法があります。したがって、ウが正解です。

- ア 解凍処理を行うことで元のデータが復元できてしまいます。
- イ 消去したデータは復元される可能性があるため、データ領域を削除、上書きするなどの対処が必要です。
- エ ファイル名を変更しても元のデータは残っているので、ファイルのデータ領域自体への対処

が必要です。

問29

《解答》ウ

HTTPSは、HTTPと暗号化プロトコルであるSSL/TLSと組み合わせて、ブラウザとWebサーバ間を暗号化して通信を行います。したがって、ウが正解です。

ア WAFの機能で実現できることの説明です。

イ、エ パケットフィルタリング型のファイアウォールの機能で実現できることの説明です。

問30

《解答》エ

リバースプロキシは、Webサーバへのアクセスを代行して受け付け、Webサーバに中継します。したがって、エが正解です。

ア DMZ (DeMilitarized Zone) は、インターネットと内部ネットワークとの間に作成する中間のネットワークです。

イ フォワードプロキシは、通常のプロキシサーバのことで、クライアントから受け取ったリクエストをインターネットに中継する仕組みです。

ウ プロキシARPは、他のホストに対するARP要求に対して代わりにARP応答する仕組みです。

問31

《解答》エ

不正アクセス禁止法は、不正アクセスを規制する法律です。不正アクセスは、実際の被害を与えなくても、不正アクセスを行うだけで犯罪となります。したがって、エが正解です。

ア インサイダー取引の説明です。

イ 不正指令電磁的記録に関する罪(ウイルス作成罪)に該当する行為です。

ウ 著作権法に違反する行為です。

問32

《解答》ア

個人情報とは、氏名、住所、メールアドレスなど、それ単体もしくは組み合わせることによって個人を特定できる情報のことです。したがって、アが正解です。

イ、ウ 個人を識別できる情報は、個人情報に該当します。

エ 個人を特定できる情報ではないので、個人情報ではありません。

問33

《解答》エ

2011年に改正された刑法で新たに追加された不正指令電磁的記録に関する罪(ウイルス作成罪)は、マルウェアなどの不正な指示を与える電磁的記録を作成、提供することを処罰する法律です。ウイルスであることを知って保管した場合には、ウイルス作成罪に該当するので、エが正解です。

ア ウイルス作成罪は、「正当な理由がないのに」ウイルスを作成した場合に適用されるものです。

ウイルス対策ソフトの開発、試験などは正当な理由となるので、罪とはなりません。

イ ウイルス作成罪は、ウイルスの作成・提供に対する犯罪なので、ウイルスだと知らないままウイルス感染させた場合は対象となりません。

ウ ウイルス対策組織へウイルスを提供することは正当な理由となるので、罪とはなりません。

問34

《解答》ウ

電子署名法では、電子署名に対し、押印と同様の効力があることを認めており、民事訴訟において電子署名を活用することができます。したがって、ウが正解です。

ア 電子署名技術は、PKI (Public Key Infrastructure : 公開鍵認証基盤) 技術をベースにしていることが求められるので、公開鍵暗号技術を使用します。

イ 電子署名は、電磁的記録に対する署名です。

エ 政府運営以外に、特定認証業務の認定を受けた第三者機関の認証局も使用できます。

問35

《解答》ウ

不正競争防止法は、事業者間の不正な競争を防止し、公正な競争を確保するための法律です。営業秘密として保護を受けるためには、「秘密管理性(秘密として管理されていること)」「有用性(有用であること)」「非公知性(公然と知られていないこと)」の三つを満たす必要があります。したがって、ウが正解です。

ア 特許法で保護される対象です。

イ 二次的著作物の説明で、著作権法で保護される対象です。

エ 著作権法で保護される対象です。

問36

《解答》イ

NAPT (Network Address Port Translation) とは、IPアドレスだけでなくポート番号も合わせて変換する方法です。一つのIPアドレスに対して異なるポート番号を用いることで、1対多の通信が可能になります。IPマスカレードと呼ばれることもあります。したがって、イが正解です。

ア DHCP (Dynamic Host Configuration Protocol) は、コンピュータがネットワークに接続するときに必要なIPアドレスなどの情報を自動的に割り当てるプロトコルです。

ウ PPPoE (PPP over Ethernet) は、イーサネット上でPPPを利用するためのプロトコルです。

エ パケットフィルタリングは、特定のパケットを遮断する仕組みです。

問37

《解答》ア

IPv4のIPアドレス32ビットのうち、最終8ビットの32を2進数に変換すると、「00100000」になります。「/28」は、32ビット中28ビットまでがネットワークアドレス、残り4ビットがホストアドレスであることを意味しています。問題文のIPアドレスから、ホストアドレスとして利用できる残り4ビットの範囲は「0000～1111」なので16になります。しかし、「0000」と「1111」は利用が予約されているので、 $16 - 2 = 14$ が接続可能なホストの最大数となります。したがって、アが正解です。

問38

《解答》イ

クラスごと、教科ごとの平均点を求めるためには、GROUP BY句を使用し、「GROUP BY クラス名, 教科名」と記述します。また、クラス名, 教科名の昇順に表示するためには、ORDER BY句を使用し、「ORDER BY クラス名, 教科名」と記述します。したがって、イが正解です。

問39

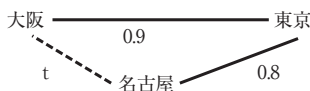
《解答》ア

ロックの掛け方には、共有ロックと専有ロックの2種類があります。共有ロック獲得済みの資源へは、別のトランザクションから新たな共有ロックの獲得は認められますが、専有ロックは認められません。専有ロック獲得済みの資源に対しては、新たに共有ロック、専有ロックのいずれも獲得することは認められません。したがって、アが正解です。

問40

《解答》エ

大阪～名古屋間のバックアップ回線の稼働率を t として図示すると、次のようになります。



東京～大阪の稼働率を0.95以上にするための稼働率 t は次の式で求められます。

$$1 - (1 - 0.9)(1 - 0.8t) \geq 0.95$$

$$t \geq 0.625$$

したがって、エが正解です。

問41

《解答》ウ

ソフトウェア資産管理に対する監査では、ソフトウェア資産の管理が適切に行われているかどうかを確認するため、ソフトウェアのライセンス証書などのエビデンスをチェックします。したがって、ウが正解です。

ア、エ ソフトウェアの信頼性に対する監査のチェックポイントです。

イ ソフトウェア導入に対する監査のチェックポイントです。

問42

《解答》エ

ITサービスを廃止する際に考慮すべき点として、廃止するITサービスの資産が他のITサービスで利用されていないか確認する必要があります。確認を怠ると、別のITサービスでインシデントが発生する可能性があるため、エが正解です。

その他の選択肢は、すでに除去された資産に対する事後対応を怠った場合の事象です。

問43

《解答》ア

縮退運転とは、システムの停止を防ぐために故障した構成品目を切り離し、システムのより重要な機能を存続させることをいいます。したがって、アが正解です。

イ バックアップの説明です。

ウ チェックポイントリスタートの説明です。

エ 更新前ログの説明です。

問44

《解答》エ

成果物を中心に、プロジェクトチームが実行する作業を階層的に要素分解したものは、WBS (Work Breakdown Structure) です。したがって、エが正解です。

ア CPM (Corporate Performance Management：企業パフォーマンス管理) は、ビジネスの状況を分析する手法です。

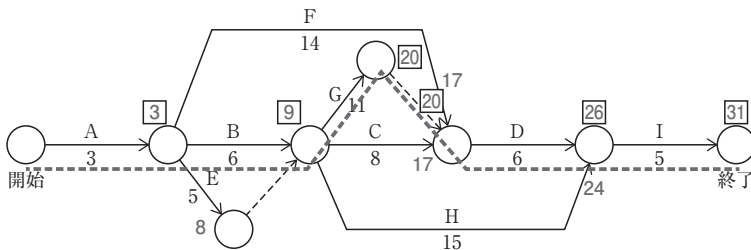
イ EVM (Earned Value Management：アーンドバリューマネジメント) は、予算とスケジュールの両方の観点からプロジェクトの遂行を定量的に評価するプロジェクトマネジメントの技法です。

ウ PERT (Program Evaluation and Review Technique) は、三点見積りという、時間見積りを確率的に行う方法で、全体スケジュールの所要期間を計算します。

問45

《解答》エ

フォワードパスを求め、クリティカルパスとそれぞれの作業の最早終了日を求めると、グレーの点線と文字で示したようになります(□で囲ったものが作業時間の合計が最も大きい経路です)。



したがって、エが正解です。

問46

《解答》ウ

組織とリーダーシップの関係では、最初はリーダーが仕事本位のリーダーシップで引っ張っていくので、図のaの状態となります。続いて、成熟度が上がるにつれ、人間関係本位のリーダーシップに移行し、図のbの状態となります。更に成熟度が進むと、構成員が自主的に行動できるようになるので図のcの状態となり、だんだんリーダーシップを必要としなくなり、図のdの状態になります。選手に戦術の立案と実行を任せるにはリーダーシップを必要としないので、図のdの状態だと考えられます。したがって、ウが正解です。

ア 図のbの状態です。

イ 図のcの状態です。

エ 図のaの状態です。

問47

《解答》ウ

平成21年4月1日から平成23年3月31日まで使用すると、2年間使用したことになります。問題の数値から、定額法での帳簿価額は次の式で求められます。

$$1,000,000 \text{ [円]} - (1,000,000 \text{ [円]} \times 0.167 \times 2 \text{ [年]}) = 666,000 \text{ [円]}$$

したがって、ウが正解です。

問48

《解答》ウ

エンタープライズアーキテクチャ (EA: Enterprise Architecture) の“四つの分類体系”は、ビジネスアーキテクチャ (BA: Business Architecture), データアーキテクチャ (DA: Data Architecture), アプリケーションアーキテクチャ (AA: Application Architecture), テクノロジアーキテクチャ (TA: Technology Architecture) です。したがって、ウが正解です。

ア システムの設計や構成のことを指します

イ ソフトウェアの設計や構成のことを指します

エ ハードウェア間の接続(バス)に関する設計や構成のことを指します。

問49

《解答》エ

要件の識別において実施する作業として、「利害関係者への要件の確認」があります。要件定義者は、定義された要件の実現可能性を十分に検討した上で、利害関係者(ステークホルダ)に要件の合意と承認を得ます。したがって、エが正解です。

ア 利害関係者の識別で実施する作業です。

イ 要件の評価で実施する作業です。

ウ 要件の合意で実施する作業です。

問50

《解答》ウ

CSR (Corporate Social Responsibility: 企業の社会的責任) を意識した調達をCSR調達といいます。自然環境、人権などへの配慮はCSRとなるので、ウが正解です。

ア コストを重視した調達です。

イ 調達のリスクヘッジに該当します。

エ 電子調達に該当します。

Q

午後 問題

問1 情報セキュリティにおけるリスクに関する次の記述を読んで、設問1、2に答えよ。

E君の所属するF社では、自社の情報セキュリティにおけるリスクを数値化して管理することになり、基準を設定して所有する情報資産のリスク評価を行うことになった。E君はこのうち、サーバX及びサーバYのリスク評価を担当した。

なお、ここでは、試行のための仮の基準と値を扱うが、それぞれに“仮”を表す文言は用いない。

〔リスクの値の算出〕

F社では、機密性、完全性、可用性のそれぞれについて、情報資産のリスクの値を、次の式で算出する。

リスクの値＝情報資産の価値×脅威^{ぜい}×脆弱性

〔情報資産の価値の評価基準〕

F社では、機密性、完全性、可用性のそれぞれから見た情報資産の価値の評価基準と値を、表1～3のとおりに設定した。

表1 機密性の評価基準と値

評価基準	値
社外に開示できる。	1
社内だけに開示できる。	2
部門内だけに開示できる。	3
必要最小限の関係者だけに開示できる。	4

表2 完全性の評価基準と値

評価基準	値
情報の完全性が失われても、業務への影響はない。	1
情報の完全性が失われても、業務への影響は小さい。	2
情報の完全性が失われると、業務への影響は大きい。	3

表3 可用性の評価基準と値

評価基準	値
定期メンテナンス以外で年間24時間までの利用停止は容認される。	1
定期メンテナンス以外で年間5時間までの利用停止は容認される。	2
定期メンテナンス以外で年間1時間までの利用停止は容認される。	3
定期メンテナンス以外で年間10分までの利用停止は容認される。	4
定期メンテナンス以外で年間1分までの利用停止は容認される。	5

〔脅威と脆弱性の判断基準〕

F社では、脅威と脆弱性の判断基準と値を、それぞれ表4、5のとおりに設定した。

表4 脅威の判断基準と値

判断基準	値
発生の可能性が低い。	1
発生の可能性が中程度である。	2
発生の可能性が高い。	3

表5 脆弱性の判断基準と値

判断基準	値
適切な管理と対策がなされている。	1
ある程度の管理と対策がなされている。	2
管理と対策が不十分である。	3

〔サーバX及びサーバY〕

サーバXでは、調達先一般情報のデータベースが稼働している。調達先一般情報とは、調達先コード、調達先の正式な名称、略称、住所、電話番号などである。

サーバYでは、取引情報のデータベースが稼働している。取引情報とは、調達先コード、購入品コード、単価、購入履歴などである。

E君は、サーバX及びサーバYの機密性、完全性、可用性のそれぞれから見た価値を評価するために、調達先一般情報と取引情報に関して、社内関連部門から聴取し、その内容を次のようにまとめた。

〔社内関連部門からの聴取内容〕

(1) 調達先一般情報

- ① 電話帳や各社のWebページで公開されている情報であるが、取引があることをF社の競合他社に知られたくない調達先もあるので、社外には公開できない
- ② この情報は、調達先との間で行っているEDI（電子データ交換）では利用していないので、誤りがあっても調達業務に与える影響は小さい。
- ③ 社員が、電話番号の確認や、挨拶状の宛先ラベルの印字に利用しているが、サーバXが利用できない場合には、代替手段での入手が可能である。

(2) 取引情報

- ① 競合する調達先をはじめ、F社の同業他社に知られてはならない情報である。また、社内でも、他部門には開示できない情報である。
- ② 情報に誤りがあれば、調達や支払などの業務に与える影響は大きい。
- ③ 営業時間内の調達オンライン入力処理、及び夜間のバッチ処理で利用されており、これらを処理するシステムは、メンテナンス以外では、年間4時間以上停止することは許されない。

〔脅威と脆弱性の状況〕

E君は、各サーバがさらされている脅威とその脅威に対するF社の脆弱性を調査し、表4及び表5の判断基準に基づいて評価した。そのうちの主なものを、表6に示す。

表6 サーバX及びサーバYの主な脅威と脆弱性の値

脅威		脆弱性	
種類	値	種類	値
ウイルス感染	3	ウイルス対策ソフト未導入	3
不正アクセス	3	アクセスコントロールの不備	2
故障	2	メンテナンス不足	3
なりすまし	2	パスワード管理の不備	2
盗聴	2	最新推奨暗号の未使用	1

〔受容可能なリスク水準〕

F社では、受容可能なリスク水準を、表7のとおりに設定した。情報資産について各リスクの値がこれらの値以下であれば、そのリスクを保有し、そうでなければ、リスク対応を行う。

表7 受容可能なリスク水準

機密性	13
完全性	15
可用性	10

〔サーバX及びサーバYのリスク評価〕

表1～5の基準、聴取内容及びサーバXとサーバYの状況から、E君は、サーバX及びサーバYに関するリスク評価を行った。F社では、評価に当たって、表1～3の評価基準では、該当する基準の値のうちで最も小さいものを選ぶことにしている。

評価結果の一部を表8に示す。

表8 サーバX及びサーバYのリスク評価(抜粋)

情報資産			脅威		脆弱性		リスク
名称	価値		内容	値	内容	値	値
	分類	値					
サーバX	機密性	a	⋮				
			なりすまし		パスワード管理の不備		f
			⋮				
	完全性	2	ウイルス感染		ウイルス対策ソフト未導入		g
			不正アクセス		アクセスコントロールの不備		h
			なりすまし		パスワード管理の不備		i
	可用性	b	⋮				
サーバY	機密性	c	⋮				
			不正アクセス		アクセスコントロールの不備		j
			⋮				
	完全性	d	ウイルス感染		ウイルス対策ソフト未導入		k
			⋮				
可用性	e	⋮					

注記 網掛けの部分は設問のため表示していない。“…”は表示の省略を示している。

設問1 表8中の a ～ k に入れる正しい答えを、解答群の中から選べ。

a ～ eに関する解答群

ア 1 イ 2 ウ 3 エ 4 オ 5

f ～ kに関する解答群

ア 4 イ 6 ウ 8 エ 9 オ 12
カ 16 キ 18 ク 24 ケ 27 コ 36

設問2 表8のサーバX及びサーバYのリスク評価に関し、F社の受容可能なリスク水準から判断されるリスク対応として適切なものを、解答群の中から選べ。なお、リスク対応No.は、表8の並び順と同じになっているものとする。

リスク対応No.	情報資産	リスク対応
1	ℓ	m
2	n	o
3	p	q

ℓ, n, pに関する解答群

ア サーバXの機密性 イ サーバXの完全性 ウ サーバXの可用性
エ サーバYの機密性 オ サーバYの完全性 カ サーバYの可用性

m, o, qに関する解答群

ア IDS（侵入検知システム）を導入する。 イ ウイルス対策ソフトを導入する。
ウ 公開鍵暗号を利用する。 エ 定期メンテナンスの回数を増やす。
オ パスワード管理を強化する。

（平成23年秋 基本情報技術者試験 午後 問4改）

問2 セキュリティインシデントへの対応に関する次の記述を読んで、設問1～4に答えよ。

E社では、外部から自社ネットワークへの不正アクセスなどの脅威に備えて、社内LANとインターネットとの接続ポイントにファイアウォールを設置している。それに加えて、よりセキュリティ強度を高めるために、ネットワーク型侵入検知システム（以下、IDSという）を図1のように設置した。

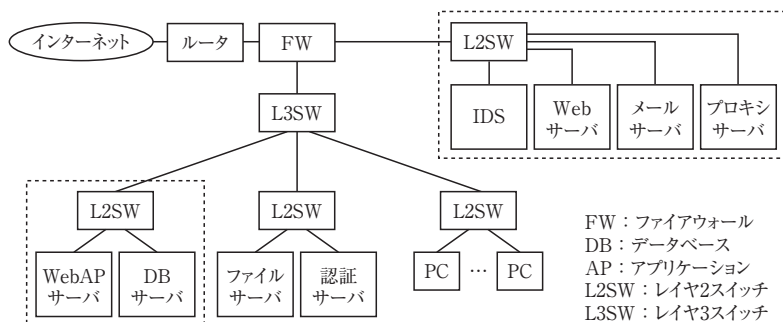


図1 ネットワーク構成

〔インシデントの発生〕

IDSの稼働開始の翌日、情報システム部セキュリティ担当のF主任が業務終了後に帰宅しようとしたところ、IDSからのアラートに気付いた。すぐに、上司であるG課長に連絡し、対応を開始した。しかし、情報システム部では、インシデント発生時に、どのような関係部署や社外の関係機関に連絡すればよいかを文書化しておらず、連絡に漏れと遅れが生じた。

アラートへの対応はG課長とF主任が中心になって実施し、対応に必要な要員を確保するのに時間を要したが、結果的に大きな問題は生じなかった。今回の事態を重視した情報システム部のH部長は、インシデント発生から対応完了までの手順に問題がなかったかを検証するために、F主任が作成したインシデント報告書を精査するとともに、G課長やF主任など、当日対応に当たった関係者から詳しい状況を聴取した。

〔インシデント対応の整理〕

関係者から聴取した内容に基づいて、H部長は、今回のインシデントへの対応を、次の(1)～(8)のように整理した。

- (1) アラートの内容から、インターネット上の特定のサイトから自社のWebサーバに対するpingの発生頻度が高く、外部からの攻撃の疑いがあると判断した。その判断に基づいて、G課長とF主任が相談の上で、初動対応を次のように実施した。

まず、危機管理担当部署など、インシデントの発生を認識する必要のある自社の関連部署に連絡した。次に、対応手順を検討し、“発生した事実の確認”、“影響の内容と範囲の調査”、“インシデントの原因と発生要因の特定”、“対策の検討と実施”の順で行うことにした。

- (2) 続いて、G課長は、アラートの内容から対応に必要な要員を選定し、情報システム部のオペレーション室に参集するよう連絡を取ろうとした。しかし、全ての情報システムの機能やネットワーク構成、及びシステム間での機能やデータの連携関係が詳細に把握できていなかったため、要員選定に非常に手間取った。
- (3) 必要な要員の参集後、G課長の指示の下で各要員が手分けして、次の(4)～(8)の作業を進めた。
- (4) アラートの発生状況や意味について事実を確認し、情報を整理した。また、インシデント発生時の状況を示す記録として、各サーバへのログイン状況、外部とのネットワーク通信状況、各サーバのプロセスの稼働状況に関する a をコピーした。
- (5) 通常業務が終了した時間帯であったので、特段の連絡は行わずに、発生したインシデントとの関連が懸念されるネットワークセグメント(図1で、破線で囲った二つのセグメント)を、外部ネットワーク及び社内LANの他のセグメントから切断した。この点に関しては、残業をしていた部署から情報システム部の担当者にクレームがあった。
- (6) インシデントによってもたらされた影響の有無とその内容・範囲を明確にするために、アラートに関連するログを調査し解析した。具体的には、サーバのシステムログからサーバへのログインやサーバ内のファイルへのアクセス状況を調査した。また、インシデントが検知されたネットワーク内の各サーバから外部に異常な通信がないかどうか、ファイアウォールとIDSのログを調査した。調査に当たっては、ログが b されたおそれがないかを事前に検証した。ログの解析作業において、各ログ間の前後関係がすぐには特定できず、作業に手間取った。
- (7) ログの調査結果と各種設定値の確認結果に基づき、インシデントの原因と発生要因の特定を進めた。その際、IDSではアノマリ検知における c があり得ることを念頭においた。特定作業の結果、アラートが発せられた原因は、E社の取引先がE社のWebサーバとの通信における応答時間をpingコマンドを使って測定する際に、pingコマンドのオプション項目を誤って指定したことによって、pingが短時間に大量に発信されたことであったと判明した。
- (8) インシデントの原因調査と並行して、社外の関係機関への連絡を準備するよう要員に指示したが、インターネット上の他サイトは連絡の対象外とした。これは、E社のサーバが d に利用されたおそれが低いと判断したからである。
- その後、インシデントの発生要因への対策、システムの復旧、再発防止策を実施した。

[H部長の意見]

インシデント対応の経緯を整理したH部長は、G課長に次のような指摘をして、対応手順を見直すよう指示した。

(1) インシデント発生時の連絡体制の整備について

- ・ 今回関係者への連絡が遅れたという事実への反省から、インシデント発生時に連絡すべき社内各部署の責任者、及び外部の機関を一覧にして連絡先を記載し、それを関係者に配布する。
- ・ インシデントの内容や発生場所に応じて、e し、連絡先とともに文書化する。

(2) 対応手順の整理について

- ・一部の部署には影響があったが、対応手順に大きな問題はなかった。しかし、対応手順をその場で検討するのではなく、インシデントの内容や発生場所ごとに手順をあらかじめ想定して、それを文書化しておくべきである。
- ・〔インシデント対応の整理〕の(5)については、今回の対応ではやむを得なかったが、セキュリティに関する攻撃を受けたおそれがあるなどの限定された状況以外では、ネットワークの切断を実施すべきではない。まず、対応手順の実施によってインシデントの影響範囲を拡大させないこととともに、インシデントの原因・影響の調査に必要となる記録を消滅させないことや業務へ影響を及ぼさないという、二次的損害の防止を考慮して対応手順を実施すべきである。また、実施に当たっては、f を怠らないことも重要である。あわせて、意思決定プロセスや判断基準をあらかじめ制定しておくことも検討すべきである。
- ・今回の対応では、〔インシデント対応の整理〕の(6)のログの解析作業において、各ログ間の前後関係がすぐには特定できず、作業に手間取るという事象が発生した。①このための対策を実施すべきである。

設問1 本文中の a ～ d に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

- | | |
|-----------------|---------|
| ア SQLインジェクション攻撃 | イ 改ざん |
| ウ 誤検知 | エ シグネチャ |
| オ 盗聴 | カ 踏み台 |
| キ マッチング | ク ログ |

設問2 本文中の e に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

- ア IDSでアノマリ検知
イ 招集すべき要員をあらかじめ選定
ウ 定期的に訓練を実施
エ ファイアウォールを導入

設問3 本文中の f に入れる適切な字句を、〔インシデント対応の整理〕(5)で示された問題点を参考にして解答群の中から選び、記号で答えよ。

解答群

- ア 影響を受けるおそれのある部署への事前連絡
イ サーバを停止する手順の確認
ウ 障害の切り分けと判断
エ 対応手順の確認

設問4 本文中の下線①について、最も適切な対策を解答群の中から選び、記号で答えよ。

解答群

- ア NTPサーバをネットワーク内に設置して、各機器の時刻を同期させる。
- イ SNMPを使って、機器の情報を収集する。
- ウ ログ解析ツールを導入する。
- エ ログのバックアップを、書換え不能な媒体に取得する。

(平成24年春 応用情報技術者試験 午後 問9改)

問3 ICカードを利用した入退室管理システムに関する次の記述を読んで、設問1～5に答えよ。

J社は、中規模のSIベンダであり、外部の協力が必要なシステム開発のときには、プロジェクトごとに協力会社と契約している。J社には、開発室と執務室があり、開発室には執務室を通じて入退室する。各室の出入口の内側と外側にICカード読取り装置が設置されており、社員と、協力会社社員（以下、協力社員という）の入退室は、入退室管理システムで管理されている。社員及び協力社員は入退室時に、ICカードを読取り装置にかざし、入室時には更にパスワードを入力することによって、出入口の扉が開錠される。また、扉が閉められると、自動的に施錠される。J社の入退室管理システムのセキュリティ要件は、次のとおりである。

〔J社の入退室管理システムのセキュリティ要件〕

- (1) 社員及び協力社員は、プロジェクトに参画している期間中だけ開発室に入室可能とする。
- (2) ICカードには、①耐タンパ性をもつものを使用し、ICカードIDだけを情報としてもつ。
- (3) ②入退室管理システムは入退室のログを収集する。
- (4) 入退室のログから、開発室又は執務室への入退室ごとの出入りした社員又は協力社員、日時、出入口が特定できる。
- (5) パスワードは8桁の数字(00000000～99999999)とする。
- (6) 有効期間中は、ICカードとパスワードによって開発室や執務室への入室ができる。
- (7) 入室時又はパスワードの変更時に、3回連続してパスワードを誤って入力した場合、開発室や執務室への入室はできなくなる。

なお、J社では、社員や協力社員が、同時に複数のプロジェクトに参画することはない。

〔入退室管理システムの説明〕

入退室管理システムが管理する、利用者情報のうち主なものを表1に、入退室情報のうち主なものを表2に示す。

表1 主な利用者情報

利用者情報	説明
利用者ID	社員の場合は社員番号を設定し、協力社員の場合は契約時に個人ごとに付与される契約番号を設定する。
ICカードID	ICカードを識別する一意のID
ICカードの状態	“仮パスワード”、“有効”、“返却”、“一時利用停止”のいずれかである。ICカードを発給したときは、“仮パスワード”を設定する。3回連続してパスワードを誤って入力した場合、“一時利用停止”になる。
入室許可の状態	“開発室許可”、“執務室だけ許可”、“入室不可”のいずれかである。
有効期間の終了日	社員の場合は、退職予定の年月日を設定しておく。協力社員の場合は契約期間に基づいて契約終了予定の年月日を設定しておく。
(上記以外の利用者情報) 氏名、有効期間の開始日、利用者区分、プロジェクト番号、パスワードなど	

注 ICカードの状態が“一時利用停止”となったICカードは、セキュリティ管理者によりパスワードが初期化される。このとき、ICカードの状態は“仮パスワード”となる。

表2 主な入退室情報

入退室情報	説明
ICカード利用日時	出入口でICカードをかざした年月日時分秒
ICカード読取り装置識別番号	出入口に設置しているICカード読取り装置を識別する一意の番号
ICカードID	出入口でかざしたICカードのID

〔入退室管理システムの運用の説明〕

セキュリティ管理者は、入室申請の受付、入退室管理システムへの利用者情報の設定、ICカードの発給を担当する。

(1) 社員に対する運用は、次のとおりである。

- (a) 社員の入社時に、入退室管理システムの運用ルールを説明した後、ICカードを発給し、パスワードを仮パスワードから変更させる。これで社員の執務室への入室が可能となる。
- (b) プロジェクトの開始時及び終了時に、プロジェクトマネージャ（以下、PMという）からの申請を受けて、開発室へのプロジェクトメンバの“入室許可の状態”の設定を変更する。
- (c) 退職時には、ICカードを返却させるとともに、“有効期間の終了日”に退職日を、“ICカードの状態”に“返却”を設定する。

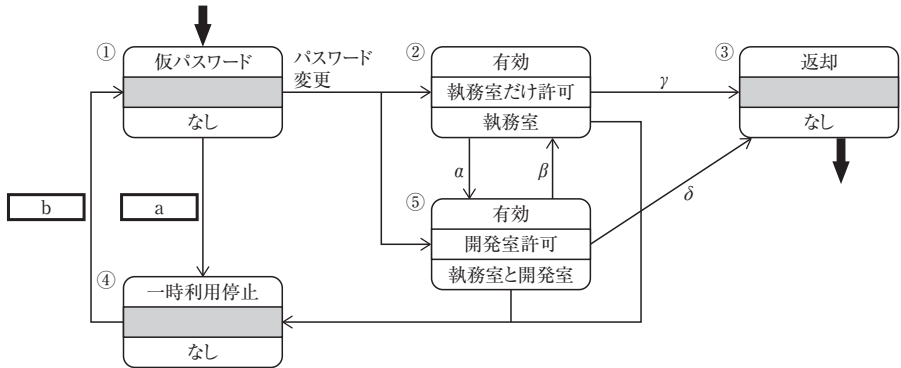
(2) 協力社員に対する運用は、次のとおりである。

- (a) プロジェクトの開始時に、PMからの申請を受けて、当該協力社員の利用者情報を登録すると同時に“入室許可の状態”を設定し、PMに協力社員用のICカードを発給する。ICカードを受領したPMは入退室管理システムの運用ルールを協力社員に説明した後、ICカードを配布してパスワードを仮パスワードから変更させる。
- (b) 契約の終了時は、協力社員に配布していたICカードの返却をPM経由で受けて、“有効期間の終了日”に契約の終了日を、“ICカードの状態”に“返却”を設定する。

(3) 利用者情報の削除処理は、次のとおりである。

- (a) “有効期間の終了日”を過ぎ、かつ、“ICカードの状態”が“返却”の利用者情報は、週末のバッチ処理でバックアップメディアに保存した上で、入退室管理システムから削除する。
- (b) 返却されたICカードは、後日再利用する。

入退室管理システムで管理する、社員を対象にした“ICカードの状態”、“入室許可の状態”及び“入室可能な部屋”の関係を表す状態遷移図を、図1に示す。



注記 網掛けの部分は表示していない。

〔凡例〕

状態番号

ICカードの状態
入室許可の状態
入室可能な部屋

図1 社員を対象とした状態遷移図

設問1 [J社の入退室管理システムのセキュリティ要件]の説明中の下線①のICカードの説明として正しい答えを、解答群の中から選べ。

解答群

- ア 一部が破損しても利用できるICカード
- イ 外部から強い衝撃があっても変形しないICカード
- ウ 内部情報に外部から不正にアクセスできないICカード
- エ 返却後に、再利用できるICカード

設問2 [J社の入退室管理システムのセキュリティ要件]の説明中の下線②のログとして収集するのが適切な情報を、解答群の中から選べ。

解答群

- ア ICカード読取り装置識別番号、ICカードID、利用者ID
- イ ICカード利用日時、ICカードID、利用者ID
- ウ ICカード利用日時、ICカード読取り装置識別番号、ICカードID、利用者ID
- エ ICカード利用日時、ICカード読取り装置識別番号、入室許可の状態

設問3 図1の a , b に入れる正しい答えを、解答群の中から選べ。

解答群

- ア 3回連続してパスワードを誤入力
- イ 社員によるパスワードリセット
- ウ 社員の入社
- エ セキュリティ管理者によるパスワード初期化
- オ 入退室管理システムの異常
- カ プロジェクトの開始
- キ プロジェクトの終了

設問4 図1を基に、最少の変更で、協力社員を対象にした状態遷移図を作成とした場合、協力社員が契約を終了して遷移する矢印として適切な答えを、解答群の中から選べ。

解答群

- ア a
- イ β
- ウ γ
- エ δ

設問5 J社では内部監査時に、開発室及び執務室の入退室に関する調査を行ったところ、入退室管理システムのログに、入室履歴のない退室履歴や退室履歴のない入室履歴が見つかった。そこで、更に調査した結果、直前に入退室した者がいるとき、扉が施錠される前に、自分のICカードを使わずに入退室する者がいることが分かった。そこで、入退室時には自分のICカードを必ず読取り装置にかざさせる対策として、教育を実施するとともに入退室管理システムで管理する現在の状態遷移を変更することにした。図1の状態番号のうち、入室履歴又は退室履歴のない者がICカードをかざして退室又は入室しようとした際に、遷移する先として適切な状態番号を、解答群の中から選べ。

解答群

- ア ①
- イ ②
- ウ ③
- エ ④
- オ ⑤

(平成25年春 基本情報技術者試験 午後 問4改)

A

午後 解答と解説

問1

情報セキュリティにおけるリスク

《解答》 34点満点

設問1 a イ b ア c ウ d ウ e ウ
f ウ g キ h オ i ウ j キ k ケ

(各2点×11)

設問2 l イ m イ n エ o オ p オ q イ

(各2点×6)

《解説》

自社で管理しているサーバXとサーバYのリスクアセスメントに関する問題です。情報資産のリスク値を算出し、優先順位を決めて、リスク保有、リスク対応を行う項目を評価していきます。リスクアセスメントの基本的な手法が問われています。

設問1

空欄a～kに関する穴埋め選択問題です。〔社内関連部門からの聴取内容〕から評価基準の値を求めていきます。

空欄a

サーバXの機密性に関する値を求めます。(1) 調達先一般情報①に、「社外には公開できない」との記述があるので、表1の評価基準「社内だけに開示できる」の値「2」が該当します。したがって、イが正解です。

空欄b

サーバXの可用性に関する値を求めます。(1) 調達先一般情報③に、「代替手段での入手が可能である」との記述があるので、表3の評価基準「定期メンテナンス以外で年間24時間までの利用停止は容認される」の値「1」が該当します。したがって、アが正解です。

空欄c

サーバYの機密性に関する値を求めます。(2) 取引情報①に、「他部門には開示できない情報である」との記述があるため、表1の評価基準「部門内だけに開示できる」の値「3」が該当します。したがって、ウが正解です。

空欄d

サーバYの完全性に関する値を求めます。(2)取引情報②に、「影響は大きい」という記述があるため、表2の評価基準「情報の完全性が失われると、業務への影響は大きい」の値「3」が該当します。したがって、ウが正解です。

空欄e

サーバYの可用性に関する値を求めます。(2)取引情報③に、「年間4時間以上停止することは許されない」という記述があるため、表3の評価基準「定期メンテナンス以外で年間1時間までの利用停止は容認される」の値「3」が該当します。したがって、ウが正解です。

空欄a～eが求められたので、続いて表6の脅威と脆弱性の値から表8を埋めると、次のようになります(計算しやすいように、実際の値を表示しています)。

表8 サーバX及びサーバYのリスク評価(抜粋)

情報資産			脅威		脆弱性		リスク
名称	価値		内容	値	内容	値	値
	分類	値					
サーバX	機密性	a : 2	⋮				
			なりすまし	2	パスワード管理の不備	2	f
			⋮				
	完全性	2	ウイルス感染	3	ウイルス対策ソフト未導入	3	g
			不正アクセス	3	アクセスコントロールの不備	2	h
			なりすまし	2	パスワード管理の不備	2	i
	可用性	b : 1	⋮				
サーバY	機密性	c : 3	⋮				
			不正アクセス	3	アクセスコントロールの不備	2	j
			⋮				
	完全性	d : 3	ウイルス感染	3	ウイルス対策ソフト未導入	3	k
			⋮				
可用性	e : 3	⋮					

リスクの値は次の式で求められます。

リスクの値＝情報資産の価値×脅威×脆弱性

空欄f～kを計算していきます。

空欄f

リスクの値＝情報資産の価値：2×脅威：2×脆弱性：2＝8

したがって、ウが正解です。

空欄g

リスクの値＝情報資産の価値：2×脅威：3×脆弱性：3＝18

したがって、キが正解です。

空欄h

リスクの値＝情報資産の価値：2×脅威：3×脆弱性：2＝12

したがって、オが正解です。

空欄i

リスクの値＝情報資産の価値：2×脅威：2×脆弱性：2＝8

したがって、ウが正解です。

空欄j

リスクの値＝情報資産の価値：3×脅威：3×脆弱性：2＝18

したがって、キが正解です。

空欄k

リスクの値＝情報資産の価値：3×脅威：3×脆弱性：3＝27

したがって、ケが正解です。

設問2

リスクの値が求められたので、表7の受容可能なリスク水準を見えます。水準値を超えているリスク値は、完全性のリスク水準15を超えている空欄g (18)、機密性のリスク水準13を超えている空欄j (18)、完全性のリスク水準15を超えている空欄k (27) の三つです。

設問2に、「リスク対応No.は、表8の並び順と同じになっているものとする」とあるので、表8の空欄g, j, kが、リスク対応No.1, 2, 3に対応します。表にすると次のとおりです。

リスク対応No.	情報資産	脆弱性
1	サーバXの完全性	ウイルス対応ソフト未導入
2	サーバYの機密性	アクセスコントロールの不備
3	サーバYの完全性	ウイルス対応ソフト未導入

空欄ℓ

「サーバXの完全性」はイが該当します。したがって、イが正解です。

空欄n

「サーバYの機密性」はエが該当します。したがって、エが正解です。

空欄p

「サーバYの完全性」はオが該当します。したがって、オが正解です。

空欄m, q

「ウイルス対応ソフト未導入」に対するリスク対応は、選択肢の中では「ウイルス対応ソフトを導入する」が適切です。したがって、イが正解です。

空欄o

「アクセスコントロールの不備」に対するリスク対応は、選択肢の中では「パスワード管理を強化する」が適切です。したがって、オが正解です。

問2

セキュリティインシデントへの対応

《解答》 34点満点

設問1	a	ク	b	イ	c	ウ	d	カ	(各4点×4)
設問2	イ								(6点)
設問3	ア								(6点)
設問4	ア								(6点)

《解説》

情報セキュリティのインシデントに関する問題です。問題に登場するE社は、ファイアウォールやIDSなどのハードウェアの設置はしているものの、インシデント発生時の対応を文書化しておらず、作業に手間取ったり他部署からクレームを受けたりするなど、見直しが多い内容になっています。

設問1

空欄a～dに関する穴埋め選択問題です。[インシデント対応の整理]を読みながら、内容を考えていきます。

空欄a

(4)中にある空欄aは、「各サーバへのログイン状況(…中略…)各サーバのプロセスの稼働状況に関するもの」です。引き続き問題文を見ると、(6)中に「ログが b されたおそれがない

かを」。(7)中に「ログの調査結果」という記述があるため、コピーするのはログであることが分かります。したがって、空欄aには「ログ」が入るのでクが正解です。

空欄b

(6)中にある「ログが b されたおそれがないかを」から、ログに対して何かされるおそれがある原因を求めることが分かります。(4)中にあるように、各種状況がログに記録されることから、攻撃者の行為の一つとしては、攻撃の痕跡を残さないように証拠隠滅を図ることが考えられます。つまり、状況が記録されているログの改ざんや消去を行います。選択肢を見ると「改ざん」があるので、イが正解です。

空欄c

アノマリ検知は、正常なパターンを登録しておき、それ以外を異常として検知する方法です。そのため、登録していない正常パターンを異常とみなしてアラートを発する誤検知が起こる可能性があります。したがって、ウが正解です。

空欄d

今回のインシデント内容は、(1)にあるように「インターネット上の特定のサイトから自社のWebサーバに対するpingの発生頻度が高く、外部からの攻撃の疑いがあると判断した」というものです。つまり、通信は外部から内部に対して行われており、サーバが不正アクセスされ、踏み台として使用されるような、内部から外部への通信ではないことが分かります。したがって、カが正解です。

設問2

〔H部長の意見〕「(1) インシデント発生時の連絡体制の整備について」に関する設問です。

〔インシデント対応の整理〕を見ると、クレームや対応に手間取った箇所がいくつか出てきます。抜き出す次のとおりです。

①情報システム部のオペレーション室に参集するよう連絡を取ろうとしたが、要員選定に非常に手間取った。〔インシデント対応の整理〕(2)

②残業をしていた部署から情報システム部の担当者にクレームがあった。〔インシデント対応の整理〕(5)

③各ログ間の前後関係がすぐには特定できず、作業に手間取った。〔インシデント対応の整理〕(6)

連絡先の文書化など、連絡体制の整備が有効な問題は、①、②です。このうち②については、空欄eの上の文章に連絡先の記載に関する記述があります。①についての対策としては、インシデントの内容や発生場所に応じて行うので、招集すべき要員をあらかじめ選定しておくことで迅速な対応ができます。したがって、イが正解です。

設問3

〔H部長の意見〕「(2) 対応手順の整理について」に関する設問です。

空欄fの前に、「業務へ影響を及ぼさない」「二次的損害の防止を考慮して対応」と記載されてい

るので、この二つの内容を実施するために怠ってはならないことを考えます。選択肢に、「影響を受けるおそれのある部署への事前連絡」があり、事前連絡によって二次的損害は防ぐことが可能です。したがって、アが正解です。

設問4

〔インシデント対応の整理〕(6)に「各ログ間」と記述があるように、ログは複数あることが分かります。また、〔インシデント対応の整理〕(4)を見ると、「各サーバへのログイン状況」「外部とのネットワーク通信状況」「各サーバのプロセスの稼働状況」と、多岐にわたります。各ログ間の前後関係を特定できるようにするためには、ログ内容の日時を正確に記録する必要があります。そのための仕組みが、NTP (Network Time Protocol) であり、ネットワーク上の機器を正しい時刻に同期させるためのプロトコルです。したがって、アが正解です。

問3

ICカードを利用した入退室管理システム

《解答》 34点満点

設問1	ウ	(6点)
設問2	ウ	(6点)
設問3	a ア b エ	(各5点×2)
設問4	エ	(6点)
設問5	エ	(6点)

《解説》

ICカードを利用した入退室管理システムに関する問題です。

日常的にICカードの利用は増えてきており、普段何気なく使っている方も多いと思います。ICカードを利用したシステムを構築する場合、ICカードのもつ特徴と、利用についてのルールを周知して運用していく必要があります。

設問1

ICカードは、内部の情報を読み出そうとすると壊れるなどの機能によって、情報の機密性を守ります。このような、物理的あるいは論理的に内部の情報を読み取られることに対する耐性のことを耐タンパ性といいます。したがって、ウの「内部情報に外部から不正にアクセスできないICカード」が正解です。

設問2

〔J社の入退室管理システムのセキュリティ要件〕(4)に「入退室のログから、開発室又は執務室への入退室ごとの出入りした社員又は協力社員、日時、出入口が特定できる」とあります。つまり収集する情報としては、「社員又は協力社員」「日時」「出入口」が該当します。表1,2から利用者情報、入退室情報を当てはめると、「利用者ID、ICカードID、ICカード利用日時、ICカード読取り装置

識別番号」が該当します。したがって、ウが正解です。

設問3

「図1 社員を対象とした状態遷移図」についての問題です。

空欄a

「仮パスワード」の状態から「一時利用停止」になる理由を考えます。表1を見ると、「ICカードの状態」の説明に「3回連続してパスワードを誤って入力した場合、“一時利用停止”になる」とあります。したがって、アの「3回連続してパスワードを誤入力」が正解です。

空欄b

「一時利用停止」の状態から「仮パスワード」になる理由を考えます。表1の注に「ICカードの状態が“一時利用停止”となったICカードは、セキュリティ管理者によりパスワードが初期化される。このとき、ICカードの状態は“仮パスワード”となる」とあります。したがって、エの「セキュリティ管理者によるパスワード初期化」が正解です。

設問4

協力社員が契約を終了した場合は、〔入退室管理システムの運用の説明〕(2)(b)に、「契約の終了時は、協力社員に配布していたICカードの返却をPM経由で受けて、“有効期間の終了日”に契約の終了日を、“ICカードの状態”に“返却”を設定する」とあります。そのため、③の“返却”が遷移先となり、選択肢はγかδのいずれかになります。〔J社の入退室管理システムのセキュリティ要件〕(1)に、「社員及び協力社員は、プロジェクトに参画している期間中だけ開発室に入室可能」とあり、協力社員も開発室に入室可能です。したがって、遷移元は⑤の“有効(開発室許可)”となり、エのδが正解です。

設問5

扉が施錠される前に、前の人について入退室を行うことを“ピギーバック”といいます。ICカードを利用し、厳密に入退室管理をしているにもかかわらず、このような入退室が行われるのは避けなければならない、教育以外にもシステム的に対応する必要があります。入退室時には自分のICカードを必ず読取り装置にかざすようにさせるためには、もし、かざさないで入退室した場合はICカードの利用を一時停止することが効果的な対策であると考えられるので、遷移先を④の“一時利用停止”にします。したがって、エが正解です。

徹底攻略 情報セキュリティマネジメント教科書 模擬問題【購入者限定特典】

著 者 株式会社わくわくスタディワールド 瀬戸美月／齋藤健一

発行人 土田米一

編集人 高橋隆志

発行所 株式会社インプレス

〒101-0051 東京都千代田区神田神保町一丁目 105 番地

TEL 03-6837-4635 (出版営業統括部)

ホームページ <http://book.impress.co.jp/>

本書は著作権法上の保護を受けています。本書の一部あるいは全部について（ソフトウェア及びプログラムを含む）、株式会社インプレスから文書による許諾を得ずに、いかなる方法においても無断で複写、複製することは禁じられています。

Copyright © 2016 Mizuki Seto/Kenichi Saito. All rights reserved.