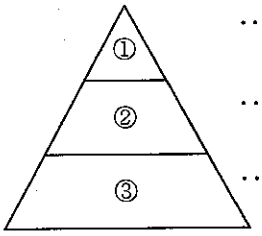
2．3　情報セキュリティ(3)　　情報セキュリティ管理

問１　【解答ア】

情報セキュリティの文書を詳細化の順に上から並べると，次のようになる。



・・・情報セキュリティ「基本方針」
：組織としての統一的かつ基本的な考え方や理念を表したもの

・・・情報セキュリティ「対策基準」
：基本方針を実践するための遵守事項や基準を記述したもの

・・・情報セキュリティ「対策実施手順」
：情報セキュリティ対策の具体的な実施手順を記述したもの

なお，基本方針と対策基準をまとめて“情報セキュリティポリシ”という場合もある。

問２　【解答ウ】

情報セキュリティマネジメントシステムにおいては，情報セキュリティマネジメントの三大要素（機密性，完全性，可用性）を維持することが求められる。このうち，“可用性”は，必要なときに，必要な資産（データ）に確実にアクセスできる特性である。したがって，「認可された利用者が，必要なときに情報にアクセスできること」が該当する。

ア：ソフトウェア製品の品質特性の一つである“機能性”の説明である。

イ：“完全性”（資産（データ）の正確さ・完全さを保護する特性）の説明である。

エ：“機密性”（認可されていない相手には，情報を非公開とする特性）の説明である。

問３　【解答エ】

情報セキュリティマネジメントシステム（ISMS：Information Security Management System）は，“計画（Plan）”，“実行（Do）”，“点検（Check）”，“処置（Act）”のPDCAサイクルで進められる。

・Ｐ（計画［Plan］）
：情報セキュリティ基本方針などを策定する。

・Ｄ（実行［Do］）
：情報セキュリティ対策基準や情報セキュリティ対策実施手順を決めて運用する。

・Ｃ（点検［Check］）
：ISMSを監視／評価する。

・Ａ（処置［Act］）
：導入したISMSを見直して改善する。（正解）

問４　【解答イ】

・リスク対策
：リスクが発生したときの対応について優先順位を決め，損失と対策費用の関係（コストパフォーマンス）などから，リスクへの対応策を決定する。

・リスク特定
：資産を調査して，発生する可能性のあるリスクを資産ごとに洗い出す。（正解）

・リスク評価
：リスクが発生した場合の損失などによる，経営上の影響範囲などを評価する。

・リスク分析
：リスクの種類や発生頻度，強度（リスクに対する強さ）などを分析する。

問5　【解答エ】

情報セキュリティポリシは，情報セキュリティに対する組織としての考え方を明文化したものである。「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。」

ア：情報セキュリティに関する規則や手順は，情報システムや管理部門ごとに策定する。

イ：情報セキュリティに関する規則や手順を社外に公開する必要はない。

ウ：情報セキュリティ基本方針も組織の状況や業務内容に合わせるべきであり，業界標準の雛形をそのまま採用する必要はない。

問6　【解答イ】

ISMS（Information Security Management System）は，企業や組織が情報セキュリティマネジメントの三大要素（機密性・完全性・可用性）を確保・維持するために，情報セキュリティポリシに基づいてセキュリティレベルの設定やリスクアセスメントなどを継続して行い，情報資産を正しく，安全に運用するための枠組みである。

a：“計画（Plan）”，“実行（Do）”，“点検（Check）”，“処置（Act）”のPDCAサイクルで進め，改善と活動を継続する。（正しい）

b：組織の経営層が情報セキュリティポリシを策定し，その基本方針に基づいて具体的な実施手順などを策定するトップダウンの活動である。

c：導入及び活動は経営層を頂点とし，組織的に取り組むべきである。（正しい）

d：改善と活動を継続し，終了することはない。

したがって，ISMSの特徴として適切なのは「a，c」である。

問7　【解答エ】

リスク回避は，リスクを避けるために，リスクの発生源となるものの使用を中止するか，代替する対応方法である。したがって，「リスクの大きいサービスから撤退した」ことが，該当する。

ア：リスク予防（リスク低減）に該当する事例である。

イ：リスク移転に該当する事例である。

ウ：リスク受容に該当する事例である。

2.3　情報セキュリティ(4)　　情報セキュリティ対策

問1　【解答エ】

社内の情報セキュリティ教育は，情報セキュリティポリシを遵守させるために社員を教育することで，情報セキュリティに関する個人の意識を高めることを目的としている。教育の「内容は，社員の担当業務，役割及び責任に応じて変更する」ことが重要である。

ア：再教育は，定期的に実施するべきである。

イ：新入社員に対しては，配属された各部署で業務を開始する前に実施するべきである。

ウ：全ての社員を対象として実施するべきである。

問2　【解答ウ】

バイオメトリクス認証（生体認証）は，人体固有の身体的特徴によって認証することである。認証対象者の身体的特徴をあらかじめ登録し，認証情報として識別する。したがって，バイオメトリクス認証の例として適切なものは，「本人の指紋で認証する」ことである。

問３　【解答ウ】

ア：ウイルスは，読み書きを行ったファイル以外に感染する可能性もあるので，ハードディスク全体の検査は定期的に行うべきである。

イ：ウイルスは，システムが稼働している間，いつでも侵入してくる可能性があるので，ウイルス対策ソフトは常に動作させて監視するべきである。

ウ：コンピュータウイルスは日々新種が発見されており，全てが既知のウイルスとは限らないので導入後もウイルス定義ファイルの更新を継続して行うべきである。（正解）

エ：プロバイダ側のウイルスチェックは有効であるが，USBメモリやCD-ROMなどから感染する場合もあるので，PCにもウイルス対策ソフトを導入するべきである。

問４　【解答ア】

・画像認証（CAPTCHA）
　：プログラムによる自動投稿を防止する技術である。画面に表示された歪んだ文字や数字を入力させ，人間が入力したかどうか判定する。（正解）

・コンテンツフィルタ
　：Webサイトのデータ（コンテンツ）をふるい分ける（フィルタリング）技術である。セキュリティの面や道徳的に問題のあるWebサイトなどを制限する。

・電子透かし
　：不正コピーなどを防止する技術である。画像などのデータに，通常は表示されない（透けて見える）作成日や著作権情報などを埋め込む。

・バイオメトリクス認証（生体認証）
　：人体固有の身体的特徴によって認証することである。許可されていない人間を，機器が設置されている部屋などに入れないようするために利用される。

問５　【解答ウ】

アクセス権設定は，情報資産（データベース等）へのアクセス権を利用者ごとに設定することで，不正アクセスによる情報の漏えい（②）や改ざん（④）を防ぐことを目的とする。

① DoS（Denial of Service）攻撃は，標的のサーバに大量のデータを送信し続け，サーバのCPU，メモリなどに過剰な負荷をかけてサービスを妨害する攻撃であり，不正侵入などを行わなくとも攻撃可能なので，アクセス権を設定しても防ぐことはできない。

③ ショルダハッキングは，パスワードを入力している人のキーボードの操作や画面に表示された情報を，肩越しから盗み見る行為であり，アクセス権を設定しても防ぐことはできない。

したがって，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は「②，④」である。

問６　【解答イ】

a：各部屋に入室を許可する社員が設定されているので，権限のある社員だけに入室を許可することができる。（適切）

b：退室は管理していないので，入室者が部屋にいた時間は記録できない。

c：入退室管理システムには全社員を登録するので，入室を試みて拒否された社員を記録することはできる。（適切）

d：退室は管理していないので，部屋にいる人数を把握することはできない。

したがって，この入退室管理システムで実現できることは「a，c」である。

問7　【解答エ】

SSL鍵マークは，データの暗号化機能とサーバ証明書による認証機能を備えたセキュリティプロトコルSSL（Security Sockets Layer）が使用されていることを表すマークである。

ア：SSLは，認証機能を備えたセキュリティプロトコルなので，サーバ証明書を確認できたことによって偽のサイトでないと判断できる。しかし，偽のサイトでないことが確認できるだけであり，ショッピングサイト運営者の財務状況が安定していることを保証するものではない。

イ：注文した商品が納品日に手元に届くかは，ショッピングサイトの運用や商品配送システムなどの問題であり，SSLで確認できることではない。

ウ：SSLでは，ディジタル署名を利用して改ざんを検出する仕組みはあるが，改ざんされた内容を修正することはできない。

エ：SSLは，データの暗号化機能を備えたセキュリティプロトコルなので，利用者などが入力した個人情報は暗号化されて送られる。その結果，途中経路で盗聴されたとしても，暗号化された内容が復号できなければ，情報が漏えいすることはない。（正解）

2．3　情報セキュリティ(5)　　アクセス制御

問1　【解答ウ】

パスワードは，利用者本人しか知らない文字列（キーワード）である。利用者が入力したIDとパスワードを使用して，システムがアクセスを許可した本人かどうか確認（利用者認証）する。パスワードの運用では，パスワードが推測されないことと，第三者に漏えいしないことに注意する。

ア：パスワードは，英数字などを組み合わせた，意味のない文字列にすべきである。英単語などを利用すると，辞書攻撃で簡単に解読されてしまう。

イ：パスワードを書いたメモなどは，人目に触れるところに置いておくべきではない。メモしたい場合には，その管理方法に十分配慮する必要がある。

ウ：パスワード漏えいの事実が明らかになった場合は，速やかに管理者に連絡すべきである。また，漏えいしたパスワードはすぐに変更するか，管理者が無効にする。（正解）

エ：パスワードは，必要十分な長さ（最低6～8文字）にすべきである。短いパスワードは，総当たり攻撃で解読されやすい。

問2　【解答ア】

・シングルサインオン
　：一度の認証で，許可されている複数のシステム（サービス，サーバ，アプリケーション）を利用できる仕組みである。（正解）

・ディジタルフォレンジックス
　：不正アクセスなどのコンピュータ犯罪が起きたとき，犯罪に関係する機器やデータを収集／分析して，法的に証拠となり得るかどうかを明らかにする技術の総称である。

・バイオメトリクス認証
　：人体固有の身体的特徴によって認証することである。許可されていない人間を，機器が設置されている部屋などに入れないようするために利用される。

・ワンタイムパスワード
　：一度しか使えないパスワード（または一度しか使えないパスワードで認証する仕組み）のことである。