セキュリティデザイナ試験　サンプル問題（解答）

No	問題	選択肢1	選択肢2	選択肢3	選択肢4	解答	説明
1	VoIPシステムに対する攻撃の記述で、「完全性」に対する攻撃に含まれるものを選びなさい	SIPサーバに対してポートスキャンを行う。	他人の音声通信パケットを収集し、通話内容を盗聴する。	大量のパケットをSIPサーバに送信する。	SIPサーバに不正侵入し、課金データを書き換える	4	完全性に対する攻撃：データの改ざん・破壊など
2	電子証明書に関して"SHA-1"は脆弱性が指摘され、今後利用されなくなるとされているが、"SHA-1"は、電子証明書を実現するの仕組みの中でどのように使われているか	証明書の持ち主の正当性検証	データの暗号化	データの改ざんの検知	サーバのFQDN、証明書の有効期間など証明書に必要な情報	1	署名検証（証明書の持ち主の正当性検証）のプロセスで、ハッシュ値を求めるのに利用されている。
3	TCPポートへの接続への応答は、ポートが開いている（サービスが動作している）場合どうなるか	SYN/ACKで応答する	RST/ACKで応答する	サーバ側からの応答はない	ICMP Port Unreachable が戻る	1	
4	SIPサーバの脅威の中で呼接続サービス妨害の対策として最も不適当な記述を選びなさい	RTPの暗号化	SIPの暗号化	音声・データネットワーク分離	端末認証	1	RTPは呼制御には用いられない
5	共通鍵暗号方式、公開鍵暗号方式の特徴についての記載のうち誤っているものはどれか	共通鍵暗号方式では暗号通信前に相手と共通の暗号鍵を共有する必要がある	共通鍵の成りすましを防止するための仕組みの一つとして電子証明書がある	公開鍵暗号方式は共通鍵暗号方式よりも一般的に暗号速度が遅い	音声トラフィックの暗号化には共通鍵暗号方式が用いられる	2	電子証明書は、共通鍵ではなく公開鍵の成りすましを防止するための仕組み
6	PC上で動作するソフトフォンを導入する際のネットワークの課題・構成について誤っているものはどれか	ソフトフォンはPC上で動作するため、L2レベルでの優先制御（CoS優先制御）が行えない	ソフトフォンを導入したPCは音声系ネットワークに接続する	音声系ネットワークの入口にSIP対応ファイアウォールを導入する	音質のQoS制御が難しい	2	一般的にPCはデータ系ネットワークに接続する
7	2015年には国内のIP電話サービスの不正利用が頻発し高額の国際電話費用が請求されることで社会問題化したが、考えられる原因として不適当な記述を選びなさい	ウィルス感染による誤動作、帯域圧迫	攻撃者がインターネット経由で不正にSIPサーバにアクセスして利用者になりすまし	利用者が外出先から外線発信できる機能を悪用	IP電話接続用ID/パスワードを入手して悪用	1	
8	NAT越え問題を解決するための方法の説明で誤ったものはどれか	ALGはデータ部の記述を解析し、ヘッダ部だけでなくアドレス情報の変換と書き換えを行う。	STUNは「STUNサーバ」にアクセスし、変換後のアドレス情報とNAT種別情報を入手する。	TURNは通信を中継するサーバをインターネットに設置する方式。	UPnPはSTUNとTURNを総括的に管理する方式。	4	4はICEの説明。
9	無線LANの脅威と対策の組合せで正しいものはどれか	盗聴と認証	不正接続と暗号化	不正APとアクセスポイント認証	盗聴・不正接続とアクセスポイント認証	3	
10	EAP認証において、認証サーバの認証を証明書、サプリカントの認証をID,パスワードなどで行う方式で正しいものはどれか	EAP-TLS,EAP-PEAP	EAP-PEAP,EAP-TTLS	EAP-TTLS,EAP-TLS	EAP-MD5,EAP-PEAP	2	
11	セキュリティ設計を行う場合の設計フローとして一般的な順序はどれか	ポリシー策定→セキュリティ設計→ 構築施工→セキュリティ評価→本運用	ポリシー策定→セキュリティ設計→ 構築施工→本運用→セキュリティ評価	ポリシー策定→セキュリティ設計→セキュリティ評価→ 構築施工→本運用	セキュリティ設計→ポリシー策定→ 構築施工→セキュリティ評価→本運用	1	
12	セキュリティポリシーは、組織や情報システムが持つ情報資産を保護する方針を定めたもの。一般的なポリシーの3階層について述べた物で誤りはどれか	対策基準は情報資産を保護するために遵守すべき行為や判断基準を示す	リスク分析は保護すべき情報資産への脅威を洗い出すこと	基本方針は基本的な考えを示す	実施手順は具体的な情報資産の保護方法を示す	2	リスク分析はポリシーを定めるための手段/ツール
13	情報セキュリティポリシの見直し手順として一般的な順序はどれか	運用上の問題点整理と分析→ 技術上の問題点整理と分析→技術情報の収集と評価→新たなリスクの整理と分析→情報セキュリティポリシーの更新	技術情報の収集と評価→運用上の問題点整理と分析→ 技術上の問題点整理と分析→新たなリスクの整理と分析→情報セキュリティポリシーの更新	新たなリスクの整理と分析→技術情報の収集と評価→ 技術上の問題点整理と分析→運用上の問題点整理と分析→情報セキュリティポリシーの更新	運用上の問題点整理と分析→ 新たなリスクの整理と分析→技術情報の収集と評価→技術上の問題点整理と分析→情報セキュリティポリシーの更新	2	