令和２年度　10 月　情報処理安全確保支援士試験　解答例

午後Ⅰ試験

問１

出題趣旨
モバイル決済が身近なものになってきた。しかし，一たび設計を誤ると，不正な決済が行われるリスクが生じる。モバイル決済でバーコード又はQRコードを使用する場合は，なりすまし対策をバーコード若しくはQRコードそのもの又はアプリケーションプログラムに行うことがポイントとなる。また，近年は，スクリーニングによってパスワードリスト攻撃の精度が向上している。攻撃者にスクリーニングを行われないような対策が必要である。 本問では，スマートフォン用決済アプリケーションプログラムの開発を題材に，メッセージ認証を用いたなりすまし対策及びスクリーニング対策を検討する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	手段	・他者のバーコードを会員番号から推測して表示する。 ・他者の会員番号を窃取してバーコードを生成し，決済する。	
		問題	・バーコードの内容が会員番号であること ・バーコードが永続的に利用できること	
	(2)	a	HMAC 値 α と HMAC 値 β の一致を検証する。	
設問２	(1)	変更する設定項目	い	
		変更後の設定内容	攻撃者の DNS サーバの IP アドレス	
	(2)	b	オ	
		c	FQDN	
		d	イ	
設問３	(1)	メールアドレスが会員登録されているかどうかで表示が異なるという挙動		
	(2)	修正すべき処理	2-b	
		修正後の処理	2-a と同じメッセージを表示する。	

問２

出題趣旨
コミュニケーション手段は多様化しているが，コミュニケーション手段としての電子メールは欠かせない。しかし，多くの電子メールは平文での送受信となっている。さらに，送信者メールアドレスの詐称によるフィッシングも起きている。これらの問題を，暗号化及びディジタル署名によって解決する手段の一つが S/MIME である。 本問では，委託先との間の，電子メールの暗号化を題材に，S/MIME を使った電子メールシステムの設計能力を問う。

設問			解答例・解答の要点	備考
設問１	(1)	a	LDAP	
	(2)	b	OCSP	
設問２	(1)	メールサーバ上では，メールが暗号化されていないから		
	(2)	c	メールサーバ	
	(3)	復号に必要な秘密鍵を意図せず削除した場合		
設問３		d	ディジタル署名	
		e	検証	
		f	ML の登録メンバ	
		g	ML	

問３

出題趣旨
情報システムのセキュリティ対策が適切に行われているかどうかを確認する手段として，専門業者による脆弱性診断サービスを受ける企業が増加してきている。診断を受ける企業において，診断効果を高めるためには，診断要件や目標を診断計画として定義することが必要である。 本問では，EC サイトへの脆弱性診断を題材に，診断を受ける企業での診断計画の策定能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	N-IPS で遮断されていた PF 診断の通信が通過するから		
	(2)	ホワイトリストに診断 PC の IP アドレスを登録する。		
	(3)	a	(a)	
設問２	(1)	b	診断用の利用者 ID	
	(2)	変更する項目	日時	
		変更する内容	診断時間を 0 時～8 時の間にする。	
	(3)	機器	本番 DB サーバ	
		変更後の設定	ホスト型 IPS のホワイトリスト設定に，診断 PC の IP アドレスを登録し，侵入検知設定を無効にする。	
	(4)	c	本番 DB サーバ	
		d	DB 管理 PC	
		e	許可	