令和５年度　春期　情報処理安全確保支援士試験　解答例

午後 II 試験

問１

出題趣旨
企業グループでは，グループ会社がそれぞれ多数の Web サイトを構築している場合がある。さらに，そうした Web サイトのセキュリティ品質を一定に保つための脆弱性診断を第三者に委託している場合と自社で実施している場合がある。 本問では，Web サイトに対する脆弱性診断を題材として，各種脆弱性に関する知識，それらを発見するためのツールの利用方法と注意点に関する知識，及び脆弱性診断を自社で実施する上での課題を解決する能力を問う。

設問		解答例・解答の要点			備考
設問１		診断対象の Web サイトの設計書を確認するという方法			
設問２	(1)	a	イ		
		b	ウ		
	(2)	c	(2-3)		
	(3)	アンケート入力 1 からアンケート入力 2 に遷移する URL の拡張機能に，アンケート確認の URL を登録する。			
	(4)	トピック検索結果の画面での検索結果の件数が 1 以上になる値			
設問３	(1)	ウ，エ			
	(2)	①	画面遷移	(A)	
			理由	同じアカウントで連続 5 回パスワードを間違えるとアカウントがロックされるから	
		②	画面遷移	(C)	
			理由	キャンペーンは 1 会員に付き 1 回しか申込みできないから	
設問４	(1)	d	HTML 内のスクリプトから cookie へのアクセス		
	(2)	偽の入力フォームを表示させ，入力情報を攻撃者サイトに送る手口			
設問５	(1)	group_code が削除されているリクエスト			
	(2)	e	JSESSIONID		
		f	group_code		
設問６	(1)	グループ各社で資産管理システムを導入し，Web サイトの情報を管理する。			
	(2)	B 社への問合せ窓口を A 社の診断部門に設置し，窓口が蓄積した情報を A 社グループ内で共有する。			

問２

出題趣旨
近年，クラウドサービスへの移行が加速する中で，セキュリティについてオンプレミスとは異なる知見が求められている。また，外部サービスとの連携が増加しているが，セキュアではない設定がされるケースも散見される。 本問では，Web サイトのクラウドサービスへの移行と機能拡張を題材として，自社システムからクラウドサービスへの移行時及び移行後におけるセキュリティに関わる設定と，外部サービスと連携する際の認可，権限設定についての分析能力を問う。

設問		解答例・解答の要点		備考
設問１		a	○	
		b	×	
		c	×	
		d	○	
		e	○	
		f	×	
		g	○	
		h	○	
		i	○	
設問２	(1)	j	ウ	
		k	エ	
		l	イ	
	(2)	{ ”system”: ”4000”, ”account”: ”11[1-9][0-9]”, ”service”: ”オブジェクトストレージサービス”, ”event”: ”オブジェクトの削除” }		
設問３	(1)	m	新日記サービス	
		n	サービスＴ	
		o	サービスＴ	
	(2)	p	(3)	
		q	(7)	
	(3)	ウ，エ		
設問４	(1)	アクセストークン要求に必要な code パラメータを不正に取得できないから		
	(2)	検証コードの SHA-256 によるハッシュ値を base64url エンコードした値と，チャレンジコードの値との一致を確認する。		
設問５	(1)	OSS リポジトリのファイル Z の変更履歴から削除前のファイルを取得する。		
	(2)	アップロードされたソースコードを承認する承認権限は，開発リーダーだけに与えるようにする。		
	(3)	X トークンには，ソースコードのダウンロード権限だけを付与する。		