平成 29 年度　春期　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
標的型攻撃メールなどによる社内 PC のマルウェア感染を起点とした，社内ネットワークからの情報漏えいや社内ネットワークでのランサムウェア感染が度々報道されている。そうした事故では，社内ネットワークのセグメントが適切に分離されていなかったことが，被害拡大の要因の一つに挙げられることが多い。 本問では，社内ネットワークへの不正侵入インシデントを題材に，ARP ポイズニングによる盗聴の原理及びそれに対するセグメント分離の効果を理解し，社内ネットワークの安全性を適切に評価する能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	a	カ	
		b	オ	
		c	エ	
	(2)	d	5	
	(3)	送信元	ケ	
		宛先	カ	
		サービス	キ	
設問 2		攻撃名	中間者攻撃	
		機器名	CRM サーバ	
設問 3	(1)	PC セグメント内に管理用 PC とサーバ間の通信が流れなくなるから		
	(2)	SYN パケット	(C) → (A)	
		SYN-ACK パケット	(A) → (B)	

問 2

出題趣旨
Web サイトは安全な状態で公開されることが望まれているので，脆弱性対策を積極的に進めている企業が増えてきている。しかし，開発者やシステム管理者の，Web アプリケーションソフトウェアの脆弱性に対する理解が不足しているために，対策しているつもりであっても脆弱性が存在した状態で Web サイトが公開されている場合がある。 本問では，クロスサイトリクエストフォージェリを題材に，Web アプリケーションソフトウェアに潜む脆弱性を理解し，対策が適切に実装されているかを評価する能力を問う。

設問		解答例・解答の要点		備考
設問 1		L 氏に確認した内容	L 氏が今日ログインしたと言っている回数	
		ログイン記録	L 氏の利用者 ID を用いた今日のログイン回数	
設問 2	(1)	a	クロスサイトリクエストフォージェリ	
	(2)	b	3	
	(3)	c	現在のパスワード	
		d	知り得ない	
	(4)	e	confirm	
		f	submit	
設問 3	(1)	カ，キ		
	(2)	g	セッションハイジャック	
	(3)	h	タグの中で利用できる属性を制限する	

問３

出題趣旨
近年，企業においても外部のクラウドサービスの利用が増加しており，企業が保有する情報資産もクラウドサービスへの移行が進んでいる。クラウドサービス上の情報資産を保護する上では，クラウドサービスでの認証とアクセス制限が重要である。 本問では，クラウドサービス側での対応が拡大しつつある SAML を用いた認証連携を題材とし，認証とアクセス制限を設計する能力について問う。

設問		解答例・解答の要点			備考
設問１		接続元 IP アドレスが F 社のグローバル IP アドレスではないこと			
設問２	(1)	a	ウ		
		b	エ		
		c	ア		
		d	イ		
	(2)	e	処理 1		
		f	処理 4		
	(3)	g	ウ		
	(4)	h	IdP		
		i	改ざん		
	(5)	認証に関する情報を利用者端末の Web ブラウザが中継するから			
設問３		交通費精算サービス	番号	(3)	
			理由	社外から IdP への通信がファイアウォールによって遮断されるから	
		グループウェアサービス	番号	(1)	
			理由	クラウドサービス側で接続元 IP アドレスの制限が行われているから	