令和３年度　秋期　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
最近のクロスサイトスクリプティング（XSS）対策は，XSS フィルタから Content-Security-Policy（CSP）に移行しているが，Web サイトを作成する技術者にはその状況があまり知られていないのが現状である。また，Web アプリケーションプログラムの脆弱性対策の負荷を避けるため SaaS の利用が進んでいるが，利用に当たっては事前のリスク分析が重要である。 本問では，Web アプリケーションプログラムを題材に，CSP を利用した脆弱性対策の能力を問う。また，SaaS への移行に当たってのリスク分析の能力とリスク対策の立案能力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	<	
		b	>	
	(2)	c	エ	
設問２	(1)	http://又は https://で始まる URL だけを出力するようにする。		
	(2)	URL と同じオリジンであるスクリプトファイル		
	(3)	スクリプト	HTML ファイル中に記載されたスクリプト	
		呼出し方法	スクリプトを別ファイルとして同一オリジンに保存して，HTML ファイルから呼び出す。	
設問３	(1)	d	ウ	
		e	ア	
	(2)	ファイルを U 社が管理する鍵で暗号化してからアップロードする。		
設問４	(1)	f	同一利用者 ID でのログイン失敗	
	(2)	アクセス元 IP アドレスを変えながら，不正アクセスを続けた場合		
設問５	(1)	g	メッセージを K サービスとの間で中継	
	(2)	h	生体認証	
		i	K サービス	
		j	アカウントを削除	
		k	アカウントを無効に	
	(3)	G サービスへのアクセスを，ファイル受渡し用 PC からのアクセスだけに限定できるから		

問２

出題趣旨
企業のネットワーク構成の在り方は，クラウドへの移行やテレワーク勤務といった事象を背景に，急激な変化が生じている。企業は，このような変化によって，新たなセキュリティ上の問題を考慮しなければならなくなっている。 本問では，テレワークにともなって発生したセキュリティインシデントを題材に，自社だけでなく，ガバナンスをきかせにくい他社を含む対応が求められる状況下での，セキュリティ対処能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	ア	
		b	イ	
		c	イ	
		d	ウ	
	(2)	e	CRYPTREC	
設問２	(1)	エ		
	(2)	B サービスのアクセス制限機能によって通信が拒否されたから		
設問３	(1)	マルウェア内に FQDN で指定した C&C サーバの IP アドレスの変更		
	(2)	C&C サーバとの通信時に DNS への問合せを実行しない場合があるから		
	(3)	f	イベントログの消去を示すログ	
	(4)	横展開機能と待機機能だけを実行していた場合		
	(5)	UTM の IDS 機能によって攻撃が検知でき，システム管理者に連絡がされるから		
設問４	(1)	g	7 月 14 日	
	(2)	h	IP リストに登録された IP アドレス	
	(3)	連携端末以外の IP アドレスを送信元とする通信記録		
	(4)	連携端末を一時的にネットワークから切り離した対応		