平成 25 年度　秋期　情報セキュリティスペシャリスト試験　解答例

午後 I 試験

問 1

出題趣旨
クロスサイトスクリプティングは昔から広く知られる脆弱性であるが，対策漏れが発生しやすく，現在でも取り組むべき代表的脆弱性である。 本問では，IPA が公表している“安全なウェブサイトの作り方”とその別冊として公表された“ウェブ健康診断仕様”を題材に，クロスサイトスクリプティング対策として行うべき実施項目と検査基準に関して出題した。Web アプリケーション開発での脆弱性への対応能力について問う。

設問			解答例・解答の要点	備考
設問 1	(1)	パターン 1	②	
		パターン 2	②	
		パターン 3	②	
		パターン 4	③	
	(2)	a	4	
	(3)	b	18	
	(4)	“http://”又は“https://”で始まる URL だけを許可する。		
設問 2	(1)	c	17	順不同
		d	24	
	(2)	e	②	
	(3)	f	GET パラメタ及び POST パラメタ	
	(4)	g	escapeHTML	
	(5)	h	26	
	(6)	i	④	
	(7)	j	out.print("document.form1.loc.value");	

問 2

出題趣旨
スマートフォンの普及によって，スマートフォン上で動作するアプリケーションが数多く公開されている。しかし，スマートフォンアプリケーションのセキュリティ対応はまだ普及しておらず，注意が必要な状況である。 本問では，スマートフォンアプリケーションを用いたサービスにおいてセキュリティ上考慮すべき点について出題した。認証の仕組み，実装上注意すべき点，及び脆弱性への対応能力について問う。

設問				解答例・解答の要点	備考
設問 1	(1)			秘密情報ではないという特性	
	(2)			イ	
	(3)			スマホアプリをリバースエンジニアリングする。	
設問 2				スマホアプリでメールアドレスを選択して，それを WebAP に送信する。	
設問 3	(1)	①	パラメタ	YoyakuCode	①と②は順不同
			内容	利用者 W の YoyakuCode	
		②	パラメタ	DateTime	
			内容	送信時とのずれが 5 分未満の時刻	
	(2)			YoyakuCode の値が AuthKey に対応する予約明細コードでないときはアプリケーションエラーを返す。	

問３

出題趣旨
クラウドサービスの利用が広がっていくとともに，クラウドサービスを利用するためのパスワードの漏えい事件も頻発しており，より強固な認証方式が求められている。 本問では，クラウドサービスを安全に利用するために有効な 2 要素認証について出題した。①2 要素認証の仕組み，②悪意の第三者による不正利用を未然に防止する又は早期に検出することができる運用手順を立案する能力について問う。 また，重要な業務におけるクラウドサービスの利用が進んでいる状況を踏まえ，クラウドサービスを利用する業務の継続について，IT の観点から事前に検討しておくべきことを問う。

設問	解答例・解答の要点		備考
設問１	方法	第三者自身の携帯電話メールアドレスを指定して申請	
	対策	管理責任者が申請者に直接申請の事実を確認する。	
設問２	理由	クッキーが有効である間，不正使用が可能だから	
	対策	C サービスの認証に使用している携帯電話は，紛失や盗難時の届出を義務化し，届出を受けたら直ちに C サービスのパスワードを変更する。	
設問３	a	プロジェクト資料を定期的にファイルサーバへバックアップ	
	b	バックアップしたプロジェクト資料を共有	
	c	データの移行方法	