平成 28 年度　春期　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
JVN を見ると，XSS（クロスサイトスクリプティング）脆弱性が後を絶たない。その上，XSS 脆弱性について，利用者が入力したスクリプトが動くだけだから，又は単にダイアログボックスが表示される程度の問題だから，悪用のおそれは低いとの誤解も多く見られる。 本問では，懸賞システムの開発を題材に，XSS 脆弱性が引き起こす被害の重大性への理解について問うとともに，XSS 脆弱性を作り込まないための対策を立案する能力を問う。さらに，CSRF（クロスサイトリクエストフォージェリ）脆弱性への対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	wana.example.jp	
	(2)	kensho.m-sha.co.jp		
	(3)	b	エ	
	(4)	c	https://kensho.m-sha.co.jp/Gamen2_2	
		d	keyword	
	(5)	懸賞メンバとしてログインしている状態		
設問２	(1)	e	ランダムな値	
		f	hidden	
	(2)	ウ		
設問３	(1)	攻撃者は，画面 2-1 を経由させずに直接画面 2-2 へアクセスさせるから		
	(2)	i	サーバサイド	
	(3)	j	URL	

問 2

出題趣旨
DMZ 上の機器に対する攻撃は継続的に行われており，不適切な設定によって，攻撃者に悪用される事例が報告されている。攻撃者に悪用されたことに気づかないでいると，自らのサイトの被害だけにとどまらず，他のサイトへの攻撃に加担させられ，加害者となることもある。 本問では，DMZ 上の機器のセキュリティ設定の点検を題材に，システム管理者が必要とするネットワークセキュリティに関する設計及び運用能力を問う。

設問		解答例・解答の要点		備考
設問１		a	オープンリレー	
		b	送信ドメイン	
設問２		c	リフレクション	
設問３	(1)	d	送信元ポート番号	
	(2)	e	外部メールサーバ	
		影響	取引先宛てのメールを，攻撃者が用意したメールサーバに転送してしまう。	
	(3)	パス名を送信しないという仕様		
設問４		変更箇所	ブラックリスト 3	
		変更内容	scanner@u-sha.co.jp を登録する。	

問３

出題趣旨
スマートフォンアプリケーションが増加している中，各種の脆弱性が見つかっており，その中でもサーバ証明書の検証不備の脆弱性は多い。これは，サーバ証明書を，その役割を正しく認識せずに，単に暗号化通信を行うために使用していることが原因だと考えられる。 本問では，スマートフォンアプリケーションの試験を題材に，サーバ証明書の検証不備に焦点を当て，検証不備を確認するための試験方法及び試験環境を設計する能力，並びにサーバ証明書の検証不備を用いた中間者攻撃についての理解を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	S サーバ	
	(2)	b	試験用 Web サーバ	
	(3)	c	試験の実施よりも前の日時	
	(4)	d	S アプリがサーバ認証エラー画面を表示する。	
設問２	(1)	e	1，2，3，4	
		f	3	
		g	1	
	(2)	SSID，暗号化方式と事前共有鍵に，公衆無線 LAN で使用されているものを設定する。		