平成 24 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Ⅱ試験

問 1

出題趣旨
Web サイトのセキュリティ対策については，ここ数年対応がとられてきているが，必ずしも万全とは言えない状況である。本問では，Web サイトの診断結果からセキュリティ対策の状況を確認し，見つかった脆弱性の修正方法，診断ツールの適切な利用方法，開発プロセスの改善方法を問う。

設問		解答例・解答の要点		備考
設問１	(1)	サーバが正常に動作しなくなるリスク		
	(2)	**検知**	サーバ停止などの異常を検知するための監視体制の整備	
		回復	サーバを元の状態に戻すための必要なファイルのバックアップ	
	(3)	a	ブルートフォース攻撃	
	(4)	b	秘密鍵	
	(5)	ポートフォワーディング		
設問２	(1)	リクエストの URL に含まれていたセッション ID を，レスポンスでクッキーとして発行していた。		
	(2)	**行番号**	74	
		理由	value 値が二重引用符で囲まれていなかったから	
	(3)	イ		
設問３	(1)	① ②	・ID ・mail	
	(2)	パラメタについては入力した値が次画面で処理される場合にだけ診断可能である点		
設問４	(1)	① ②	・システムで利用している OS やミドルウェアの脆弱性情報を定期的に収集し，必要な対応を行う。 ・自動診断ツールを最新のものに更新し，定期的に診断を実施し，必要な対応を行う。	
	(2)	チェックシートに基づきコーディング規約を整備する。		

問２

出題趣旨
無線 LAN を経由したインターネット接続形態が，昨今のスマートフォンやタブレットといった携帯可能デバイスからの接続をはじめ増えていることを踏まえ，本問では無線 LAN を題材とし，無線 LAN の導入及び，それに伴う社内ネットワークの構成変更が，情報セキュリティ管理規程や既に講じているセキュリティ対策へどのような影響を与えるのか，またその影響に対してどのように対応すべきかを問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	イ	
		b	ケ	
		c	エ	
	(2)	**情報の特性**	顧客から預かった機密データを扱うから	
		利用可能なエリア	T 社オフィス外でも通信を傍受できる可能性があるから	
	(3)	事前共有鍵の変更		
設問２	(1)	③	MAC アドレスは偽装可能だから	
		④	SSID は傍受可能だから	
	(2)	会議室 LAN からプロキシサーバへの通信を許可する。		
設問３	(1)	①	・ウイルスチェック	
		②	・URL フィルタリング	
	(2)	**EC サイトコンサルティング事業部員及び EC サイト開発事業部員のアカウント**	執務室用の無線 LAN と会議室用の無線 LAN のどちらかを選択して接続できるようにする。	
		それ以外	会議室用の無線 LAN と OA-LAN のどちらかを選択して接続できるようにする。	
	(3)	ノート PC をロックせずに放置すること		
設問４	(1)	①	**項目** 9-2	①と②は順不同
			内容 来客所有のデバイスが無線 LAN に接続されること	
		②	**項目** 14-1	
			内容 来客のインターネットアクセス時の通信ログが取得されないこと	
	(2)	来客のデバイス用のクライアント証明書を発行する負荷		
	(3)	**送信元ネットワーク**	来客 LAN	
		宛先ネットワーク	インターネット	
		通信プロトコル	①・HTTP ②・HTTP Over TLS	