平成 30 年度　春期　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
セキュリティインシデントを未然に防ぐには，新しい攻撃方法の出現や，システムの変更，業務の変更など様々な環境の変化に合わせて，企業・組織がリスクを見直し，必要となる対応をしていくことが重要である。 本問では，一般社団法人におけるセキュリティ対策の評価を題材に，脆弱性検査で検出された脆弱性や，リスクアセスメントによって新たに分かった情報漏えいリスクなどについて，評価し，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)		脆弱性の有無によってサーバからのレスポンスに違いがないから	
	(2)		スクリプトを分析し，フラグメント識別子の値の変化による挙動を確認する。	
	(3)		R ポータルが利用しているスクリプトが Cookie の値を利用している場合	
設問 2			踏み台サーバの操作記録機能によって，ログインした利用者のデスクトップ画面，実行したコマンド，及びキーボード入力を記録する。	
設問 3	(1)	a	WebAP サーバ	
		b	DB サーバ	
		c	ODBC	
		ルール	9	
	(2)		人事総務課の職員が踏み台サーバを経由して DB サーバに共通管理者アカウントでログインする行為	
	(3)	d	2	
設問 4	(1)	e	製作パートナに渡す CCI の数	
	(2)	f	CC をインストールした PC を協力者宛てに輸送	
	(3)	g	DRM サーバへの通信を製作パートナのグローバル IP アドレスからだけに制限する	

問２

出題趣旨
Web サイトのセキュリティは，向上してきてはいるものの，セキュリティインシデントはいまだに後を絶たない。脆弱性診断の実施や，設計，実装，テスト及び運用のガイドラインの利用といったセキュリティ対策に改善の余地があると考えられる。 本問では，Web サイトのセキュリティを題材に，Web サイトで発生したセキュリティインシデントについて調査し，対策を立案する能力，脆弱性診断を実施する場合に Web サイトの仕様に基づいて診断手順を検討する能力，及び診断結果から得られた知見を基にガイドラインを改善する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	攻撃に使われる文字列が POST データ内に含まれている場合		
	(2)	a	Web サイト Y の全ファイルと比較	
	(3)	公開鍵認証方式		
設問２		b	Web サイトで使用している OS，ミドルウェア及び WF の名称並びにそれぞれのバージョン情報	
設問３		c	ディレクトリ	
		d	クロスサイト	
		e	HTTP	
		f	ジャッキング	
設問４	(1)	g	30	
		h	0	
	(2)	i	イ	
	(3)	j	（う）の操作を実行するときに，code の値を限定商品の値に書き替える	
	(4)	k	権限が異なる複数の	
		l	許可されている操作の違い	
設問５		作業の妥当性を確認できる詳細なレビュー記録を委託先が提出していること		
設問６		脆弱性の作り込み原因を調査して，注意すべきポイントを追加する。		