令和４年度　春期　情報処理安全確保支援士試験　解答例

午後Ⅰ試験

問１

出題趣旨
システム開発においては，要件定義からテストまでの全てのプロセスでセキュリティ対策が必要であることは広く認識されている。一方で，アクセス制御における設計上の考慮不足や実装の不備による情報流出の被害事例が後を絶たない。たとえアクセス制御が単純なものであっても，問題が発生しているのが現実である。 本問では，情報共有用 Web アプリケーションプログラム開発のセキュリティ対策を題材として，システム開発の設計，実装，テストの各プロセスにおける脆弱性の分析及び修正に関わる能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	ア		
	(2)	プレースホルダ		
	(3)	a	改行コード	
設問２	(1)	クエリ文字列の id に，未参加のプロジェクトのプロジェクト ID を指定する。		
	(2)	・プロジェクトを示すパラメタを外部から指定できないから ・セッション情報からプロジェクト ID を取得するから		
	(3)	b	ウ	
	(4)	c	stmt	
設問３		d	情報番号 = ? AND プロジェクト ID = ?	

問２

出題趣旨
IoT 機器の普及に伴い，利用者が専門知識なしに容易に機器を設置できるようになる中，開発者がセキュリティを考慮していなかったり，利用者が脆弱性修正プログラムを適用していなかったりするケースが増えている。 本問では，ルータや NAS を題材として，IoT 機器のインターネット接続に使われる技術，仕組みを理解するとともに，脆弱性を作り込んでしまうことの多い Web 機能についてセキュリティの観点から正しく実装する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	ア	
		b	エ	
	(2)	外部から LAN 側への通信の許可設定が変更される。		
	(3)	PC からのファイル操作ではアクセスできない領域のファイルが暗号化されたから		
設問２	(1)	c	パストラバーサル	
	(2)	d	OS コマンドインジェクション	
	(3)	e	ア	
		f	ウ	
		g	イ	
設問３	(1)	POST メソッドで送信したボディがアクセスログに残っていなかったから		
	(2)	sudo コマンドの設定ファイルで，tar コマンドのオプションを受け付けないように設定する。		
設問４		h	・noindex ・none	

問３

出題趣旨
近年，スマートフォンを用いた決済において不正利用事件が多発している。IPA が公開している“情報セキュリティ 10 大脅威”の個人部門では“スマホ決済の不正利用”が 2020 年度，2021 年度で 1 位となっており，サービス提供者による対策が望まれている。 本問では，スマートフォン向け QR コード決済サービス用プログラムの開発を題材として，不正利用が発生するリスクとサービス提供者での対策について，セキュリティの観点での対応力を問う。

設問		解答例・解答の要点		備考
設問１		a	イ	
		b	ア	
設問２	(1)	① ②	・漏えいしている口座番号と暗証番号を悪用する方法 ・口座番号と暗証番号をだまして聞き出し，悪用する方法	
	(2)	c	写真	
	(3)	d	ウ	
		e	イ	
	(4)	f	・署名用電子証明書の有効性 ・署名用電子証明書の失効の有無	
	(5)	g	そのランダムな数字を紙に書き，その紙と一緒に容貌や本人確認書類を撮影	
設問３	(1)	スマートフォンを盗まれた場合		
	(2)	Q アプリの起動時に，PIN コードで利用者を認証する機能		