令和４年度　秋期　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
製品開発においては，設計・開発時に十分なセキュリティ対策を行うことが重要である。脆弱性単体では発生し得る被害が小さいように見えたとしても，他の脆弱性と組み合わせられることで，より大きな被害が発生することもある。 本問では，IoT 製品の開発を題材に，開発者として脆弱性単体だけでなく，複数の脆弱性の組合せによって生じるリスクを特定する能力，及びアプリケーションプログラムのセキュリティ対策を策定する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	DNS キャッシュポイズニング	
	(2)	b	エ	
	(3)	権威 DNS サーバからの応答よりも早く到達する。		
	(4)	サーバ証明書を検証し，通信相手が W サーバであることを確認する実装		
	(5)	c	コードサイニング	
設問２		d	シェルが実行するコマンドをパラメータで不正に指定できて	
設問３	(1)	攻撃リクエストを POST メソッドで送信させるスクリプトを含むページを表示させる仕組み		
	(2)	e	推測困難である	
設問４		脆弱性 A	ア	
		脆弱性 B	オ	

問２

出題趣旨
日々発見される新たな脆弱性に対し，運用者が脆弱性の影響を確認し，必要な対策を行うことは重要である。しかし，全ての脆弱性が攻撃者より早く発見され，運用者が必要な対策を行えるとは限らないので，攻撃者が未修正の脆弱性を悪用するリスクについても考慮しておく必要がある。 本問では，ソフトウェアの脆弱性に起因するセキュリティインシデントへの対応を題材に，攻撃者の痕跡を調査し，影響を把握する能力及びセキュリティ侵害を前提とした適切なアクセス制御を設計する能力を問う。

設問		解答例・解答の要点		備考
設問１		a	a3.b3.c3.d3	
設問２	(1)	run プロセスの親プロセスが T ソフトのプロセスであるから		
	(2)	b	13:04:32	
		c	13:05:50	
		d	a8.b8.c8.d8	
		e	LDAP	
		f	JExp	
設問３	(1)	ログ出力処理する文字列中に攻撃文字列が含まれれば悪用可能だから		
	(2)	会員サーバからインターネット宛ての LDAP 通信が許可されていないから		
設問４		g	予約サーバ	
		h	SNS 投稿用のサーバの URL	
		i	全て	

問３

出題趣旨
OSS を用いたソフトウェア開発が一般化している。一方，悪意あるプログラムや脆弱性をもつプログラムが OSS に混入する可能性が高まっている。事実，情報セキュリティ 10 大脅威 2022 の“組織”向け脅威にサプライチェーンの弱点を悪用した攻撃やゼロデイ攻撃がランクインしている。そこで，そのような事象を想定したインシデントハンドリングの体制及び手順を検討しておくことは重要である。 本問では，オンラインゲーム事業者でのセキュリティインシデント対応を題材に，インシデントハンドリングを行う能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	376	
	(2)	prog というファイルをダウンロードし，実行する命令		
	(3)	b	一時ディレクトリ内のログ	
	(4)	ゼロデイ攻撃		
設問２	(1)	レジストリサーバに固有のレスポンスヘッダ		
	(2)	上書きされたイメージを削除する。		
設問３	(1)	c	a3.b3.c3.d3	
	(2)	d	エ	
	(3)	別の IP アドレスを攻撃者が用いる場合		
	(4)	e	オ	