平成 29 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
組織及び個人において，ランサムウェアの被害が拡大している。業務継続の観点から，これまでのマルウェア対策に加えて，バックアップやアクセス権限設定などの対策も見直しが必要となっている。 本問では，業務システムにおけるランサムウェア感染のセキュリティインシデントを題材に，ランサムウェアの基礎知識とともに，インシデントが発生した場合の初動対応や再発防止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		イ		
設問 2	(1)	a	オ	
		b	エ	
	(2)	バックアップ終了時刻		
	(3)	営業用 PC の設定	D サーバ上の共有フォルダをネットワークドライブとして割り当てる。	
		ランサムウェア X の特徴	ネットワークドライブ上のファイルも暗号化の対象となる。	
	(4)	D サーバと G サーバのファイルの暗号化		
設問 3	(1)	c	可	
		d	可	
		e	可	
		f	不可	
		g	可	
		h	不可	
	(2)	復号に必要な共通鍵や秘密鍵が検体に含まれていないため		
	(3)	PC 内で一時的に作成されたメモリ上の共通鍵が消えてしまうため		
設問 4		共有フォルダのバックアップデータも暗号化されてしまい復元できなくなる。		

問２

出題趣旨
クロスサイトスクリプティングと SQL インジェクションの脆弱性は，現在でも数多く報告されている。また，オープンリダイレクタの問題は，情報漏えいの被害には直接つながらないものの，Web アプリケーションを設計・構築する上で重要なトピックである。 本問では，Java／Servlet を用いた Web アプリケーションのセキュアプログラミングを題材に，脆弱性への対処方法について開発者の観点で確認する。また，Web アプリケーションでの通信を TLS とする際に気を付けるべき，Secure 属性と HttpOnly 属性についても取り上げている。

設問		解答例・解答の要点		備考
設問１	(1)	ア	9	
		イ	11	
		必要な全てのコード	カ，ア，イ，ウ	
	(2)	21，22，23		
	(3)	ウ		
設問２	(1)	a	エ	
		b	イ	
	(2)	認証後のリダイレクト先の URL を，W システムの FQDN のものに限定する。		
設問３	(1)	セキュリティ検査を本番システムに対し行うこと		
	(2)	ブラウザによっては XSS 攻撃を遮断する機能をもつから		
	(3)	W システムで当該脆弱性に対処する前に始まる攻撃によって，セキュリティ侵害されてしまうリスク		

問３

出題趣旨
インターネットにおいて，SSL/TLS は欠くことのできない技術であり，Web サービスをはじめとして，各種サービスの基盤として利用されているが，SSL/TLS を利用する場合には注意点がある。サーバ証明書の鍵の漏えい，つまり危たい化は起こり得るし，また，新しく発見された攻撃方法によって対応が求められる場合もある。 本問では，サーバの鍵の危たい化を題材に，暗号技術に関する基礎的知識，SSL/TLS についての基礎的知識，及び SSL/TLS を正しく設定し，利用し，運用する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	コ	
		b	カ	
		c	オ	
		d	イ	
	(2)	正規の EC サイトの URL でアクセスしたときに，偽の EC サイトに誘導する。		
	(3)	エ		
設問２	(1)	ア	利用	
		イ	失効	
	(2)	①	・鍵が危たい化した Web サイトの FQDN	
		②	・鍵が危たい化したと思われる日時	
	(3)	e	鍵ペア	
設問３	(1)	SSL3.0 を利用しない設定にする。		
	(2)	ウ，オ		
	(3)	エ		
	(4)	ドメイン認証証明書ではサーバの運営者が C 社であることを確認できないから		