平成 21 年度　春期　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
公開鍵証明書を必要とするシステムを構築する際に，商用 CA を利用する場合と，自営 CA を利用する場合があるが，いずれの CA を利用すべきかの判断基準がないままに決定されることがある。 本問では，自営 CA を利用する場合に注意すべき点を明確にし，安全な PKI を構築できる能力を問う。

設問		解答例・解答の要点		備考
設問１		**a**	1,024	
		b	SHA-1	
		c	ハッシュ値	
		f	ルート	
設問２		**問題**	社内ネットワークに接続されないと，ウイルス定義ファイルが更新されない。	
		対策	インターネット上のウイルス定義ファイル配布サーバからも更新できるように，PC の設定を変更する。	
設問３		① ②	・テレワーク PC の紛失，盗難対策を行う。 ・テレワーク PC を他人に貸与しない。 ・テレワーク PC 以外に秘密鍵及び証明書を導入しない。 ・テレワーク PC の利用者パスワードを堅ろうなものにする。	
設問４		電子署名の対象のデータを改ざんした上で，そのハッシュ値から，推測した秘密鍵で署名を生成し，本来の所有者と偽って送信する。		
設問５	**(1)**	グループ販社の発注担当者の証明書が偽造され，偽の注文票が送られる可能性がある。		
	(2)	**d**	(イ)	
		e	(ケ)	
	(3)	・CA において，利用者の秘密鍵を厳重に管理する。 ・鍵ペアと証明書の送付後に，CA では秘密鍵を削除する。		
設問６		**問題**	署名の正当性を確認できない。	
		理由	A 社 CA のルート証明書を導入していないから	

問2

出題趣旨
情報セキュリティの実現に当たっては，適切なセキュリティ技術を選択するとともに，組織に適合したセキュリティポリシを適用し，その継続的な改善を図ることが望まれる。 本問では，衣料小売業者における情報セキュリティの見直しを題材に，法的要求事項や情報セキュリティ標準の知識，セキュリティ検査の技法，Web アプリケーションの保護の手法などについて問う。

設問		解答例・解答の要点	備考
設問1	(1)	a　マネジメントレビュー　又は　情報セキュリティ委員会	
	(2)	・開発の要件としてセキュリティ要件を提示していない以上，成果物に脆弱性が発見された場合でも受け入れざるを得ない。 ・発見された脆弱性に対する改修費用を開発元と委託先のどちらが負担するかでトラブルが生じる。	
設問2	(1)	b　事業継続	
		c　NTP	
	(2)	ウイルス対策ソフトの動作ログを採取し，レビューを行う。	
	(3)	システムで利用されるサービスのポート番号以外のポートがオープンになっていないかどうか。	
	(4)	災害の発生時にシステムのデータとバックアップ媒体上のデータが同時に被災する可能性がある。	
	(5)	管理を行っているシステムを自ら検査することになるから	
設問3	(1)	Web では，一つの脆弱性に対して攻撃を引き起こす可能性のあるアクセスのパターンが多岐にわたるから	
	(2)	WAF 単独では取りこぼしが発生し得るので，脆弱性が修正されない場合には攻撃を受ける可能性が高い点	
設問4	(1)	d　エ	
	(2)	e　トランザクションログに対して参照可能な利用者を制限する	
設問5		・追加した対策の有効性を内部監査によって確認し，改善すべき点があれば改善計画を立てて改善を行う。 ・新たに追加された対策を加味してリスク分析を実施する。 ・新たに追加された対策についての有効性の評価を行う。	