平成 22 年度　秋期　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
クラウドコンピューティングの広がりによって，アプリケーションがサービスとして提供される機会が増えている。そのため，アプリケーション全体のセキュリティ対策をより適切に実施することが求められる。 本問では，アプリケーションサービスの開発プロジェクトを題材として，安全なシステムの開発に必要な開発工程，アプリケーション実装及び共同利用型のシステムにおけるデータ分離の知識を問う。また，開発プロジェクトでの組織的な問題を解決する能力を問う。

設問		解答例・解答の要点		備考
設問１		a	ア	
		b	イ	
設問２	(1)	修正に期間が掛かり，本番稼働が延期となる可能性があるから		
	(2)	セキュリティ要件が正しく設計に反映されているかどうかをレビューする。		
	(3)	開発ガイドライン及びコーディングルールに基づきコーディングされていることを確認する。		
設問３	(1)	【選択した従業員の利用者 ID】を表すリクエストパラメタの値としてほかの店舗の利用者 ID を与える。		
	(2)	【選択した従業員の利用者 ID】の値がログイン中の利用者と同じ店舗の従業員の利用者 ID かどうかをチェックする。		
設問４	(1)	データベースのテーブルとアカウントを顧客ごとに分離し，アクセス権を設定する。		
	(2)	・開発委託先の成果物に対して，委託先のレビューに加えて，X 社でも受入検査を詳細に実施する。 ・チェックリストの各項目を判定する基準を示し，その判定結果と根拠を提出させる。		
設問５	(1)	c	ア	
	(2)	d	ファイアウォールで，インターネットからの TCP ポート番号 8080 への通信を拒否する。	
	(3)	X 社の標準開発プロセスに脆弱性情報の収集と管理責任を規定する。		

問２

出題趣旨
本問は，組織内の認証システムの統合を進める上で，情報システム部門が解決すべき課題を幅広く扱っている。 認証及び関連技術に関しては，旧来の技術から最新の技術までを対象にして出題した。認証システムを統合する上での，基本的な設計能力及び重要な課題の一つであるスケジューリングに関する能力を問う。旧認証システムである A-SSO システムを利用しているシステムが，新方式である統合認証システムに連携し終わるまで A-SSO システムを廃止できず，A-SSO のサービスを継続させなければならないということへの“気づき”を確認する。また，A-SSO のサービスを継続するための阻害要因を状況から見いだす能力に加えて，連携しているシステムのリプレース時期を見据え，A-SSO の廃止時期の判断を問う。

設問		解答例・解答の要点		備考
設問１		b	オ	
		c	イ	
		d	ウ	
		e	カ	
設問２	(1)	チャレンジとレスポンスのペアを盗聴し，正規のレスポンスを用いてリプレイ攻撃によるなりすましをする。		
	(2)	a	時刻同期	
設問３	(1)	所管部門の異なる A-Web アプリのすべてに同一の暗号化鍵を配布していること		
	(2)	暗号化及びディジタル署名した SAMLResponse メッセージを用いて，IdP から SP へ認証情報を転送している。		
設問４	(1)	管理フォーマットを一つにし，IDM でパスワードを一元的に管理し，それを各情報システムが参照する仕組みを導入した。		
	(2)	SaaS 型サービスのアカウント管理と運用を，必要に応じて，A 社から切り分けることが可能となる。		
設問５	(1)	f	2014	
		S チームが判断する理由	A-SSO システムと連携した情報システム群のリプレースがすべて完了するから	
	(2)	g	A-SSO システムが稼働するサーバマシンのベンダサポートが 2012 年末で切れる	