平成 27 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
シンクライアント技術は，データがクライアントに残らないことから，情報漏えい対策の一つとして広く採用されている。ただし，その設計においては，セキュリティ以外の要件も踏まえる必要がある。 本問では，マルウェアによる情報漏えいへの対策，シンクライアント技術及びその他のセキュリティ対策技術を題材に，セキュリティ要件と業務要件及びパフォーマンス要件とのバランスを考慮した，OA システムの設計能力を問う。

設問		解答例・解答の要点				備考
設問 1	(1)	(a)	1，2，3			
		(b)	1，3，7，8，9			
		(c)	1，10，11			
	(2)	構成要素	TC サーバ			
		通信	2，3，10，11			
設問 2	(1)	①	・通信が暗号化されている場合			
		②	・ファイルが暗号化されている場合			
	(2)	クライアントアプリケーションのプロセスが起動される度に，IP アドレスが変わるので，認証済みのほかの利用者として認証されてしまう可能性があるから				
	(3)	IA 用 TC サーバ				
	(4)	OA 用 TC サーバ				
	(5)			a 群	b 群	同じ群中の組合せとする
		Web サイトのファイルを閲覧した場合	送信元	IA 用 TC サーバ	IA 用 TC サーバ	
			宛先	ファイルサーバ	グループウェアサーバ	
			プロトコル	Windows ファイル共有プロトコル	グループウェア独自プロトコル	
		受信メールの添付ファイルを開いた場合	送信元	OA 用 TC サーバ		
			宛先	インターネット上の Web サーバ		
			プロトコル	HTTP 及び HTTPS		
設問 3	(1)	b，c，f，g				
	(2)	Web サイトのファイルを閲覧した場合		海外支店 X 用 TC サーバ		
		受信メールの添付ファイルを開いた場合		海外支店 X 用 TC サーバ		
設問 4	(1)	476				
	(2)	ア，ウ，オ，キ，ク				
設問 5		セキュリティ管理の状況を客観的に監査できないという不具合				

問２

出題趣旨
近年，企業からの重要データの漏えい事件が世間を騒がせる機会は，ますます増加する傾向にある。 本問では，データの管理に焦点を当て，活用が広がるクラウドストレージと暗号技術，その他の技術的手法，運用上の手法などを組み合わせて，適切なセキュリティ環境を構築するための知識と能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	マルウェア感染ファイルが複数の利用者の同期用フォルダ間で自動同期される。		
	(2)	マルウェア感染ファイルの発見時に利用者に警告を発する機能		
設問２	(1)	a	ク	
		d	ア	
		e	オ	
		f	キ	
	(2)	b	営業秘密	
		c	公然と知られていない	
設問３	(1)	g	OS	
		h	暗号化	
	(2)	平文が同じブロックは同じ暗号文になるので，暗号文から平文を推測されやすい。		
	(3)	i	1	
		j	24	
		k	1	
		l	1	
		m	5	
	(4)	n	CBC モード	
		o	OFB モード	
設問４	(1)	鍵は，サーバごとに生成し，Q サービス内で管理される。		
	(2)	鍵が危殆化しても，当該鍵が利用されるフォルダ以外には影響がない。		
	(3)	①	・ファイルの名称	
		②	・おおよそのファイルサイズ	
	(4)	p	9	
		q	62	
		r	2	順不同
		s	31	
		t	8.9	
設問５	(1)	暗号化フォルダに登録されたファイルは，復号した後で，マルウェアスキャンを行うようにする。		
	(2)	場合	利用者が，暗号化していないファイルを Web ブラウザで登録した場合	
		修正内容	暗号化されていないバックアップのファイルを自動で削除する。	
設問６		委託先のデータ管理の実態を監査によって把握して監督する。		