

平成 21 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 試験

問 1

出題趣旨	
セキュリティポリシーや対策標準があっても、それらの遵守が現実には思うようになされないことが多々ある。 本問では、セキュリティに関する規定からシステムまでの総合的な見直し力を問うために、電子メールからの情報漏えい対策を題材とした。システム構築に関しては、現状のネットワーク構成を理解した上での対応能力を問う。昨今、ビジネスですっかり身近になった携帯電話を採り上げることによって、受験者の周囲でも同様の問題に取り組むきっかけとしてもらいたい。	

設問		解答例・解答の要点		備考	
設問 1		a	ウ		
		b	イ		
設問 2	(1)		5.9(2)	順不同	
			5.9(3)		
			5.13(5)		
	(2)	情報	顧客の電話番号 又は アドレス帳 又は メールアドレス		
		対策	サーバにアドレス帳のバックアップをとり、漏れた電話番号が分かるようにする。		
設問 3		・ 管理者がリモートから携帯電話の保存内容を削除できる機能 ・ 管理者がリモートから携帯電話をロックできる機能			
設問 4	(1)	携帯電話の電子証明書のコモンネーム			
	(2)	箇条と項番	5.9(2)		
		対策	・ 電子証明書を利用するための暗証番号が有効であることを携帯電話 1 台ずつについて上司が確認する。 ・ 携帯電話の端末操作制限の暗証番号が有効であることを携帯電話 1 台ずつについて上司が確認する。 ・ 携帯電話の端末操作制限機能やデータ保護機能を情報システム部門が有効にしてから貸与する。		
	(3)	サーバ間	Z 社提案ポータル サーバと メール サーバの間		
		プロトコル	IMAP		
設問 5		業務目的のメールを会社貸与の携帯電話の従業員用メールアドレスに転送することを禁止する。			

問 2

出題趣旨	
Java アプレットを用いたシステムが利用されるようになって久しい。 本問では，実行環境を OS とは別にインストールする Java のような技術を利用したシステムにおけるセキュリティを考える。特に，要素技術や実現方法の知識からバージョン管理といった様々なレベルの課題に対し，幅広く対処する能力を問う。	

設問	解答例・解答の要点		備考
設問 1	a	エ	
	b	ウ	
	d	ア	
	e	カ	
設問 2	(1)	c ウ	
	(2)	(ア)	
設問 3	(1)	X システムのクライアント PC 上のブラウザでインターネットの Web ブラウジングを行うとき	
	(2)	・入力チェック機能 ・チェック結果を利用者へ通知する機能 ・アップロードされたファイルを消去する機能	
設問 4	(1)	新しいバージョンの JRE で，本体モジュール，ファイル受信モジュールと入力チェックアプレットの動作確認	
	(2)	X システムのサーバで利用する JRE では，当該脆弱性を悪用した Java のクラスを実行する可能性がないことについて，適切に記述していること	解答の要点を示す

問 3

出題趣旨	
多目的型の IC カードを用いた入退室管理やログイン認証を導入する企業が増えている。 本問では，IC カードの導入に際して必要となる，IC カード自体のセキュリティ，IC カードの発行と運用，及び IC カード認証に関する知識と応用力を問うとともに，最近導入事例が増加しつつある認証プリントに関する理解度を問う。	

設問	解答例・解答の要点		備考
設問 1	(1)	ア 正規の IC カードだけが使用できること	
	(2)	イ 耐タンパ性	
	(3)	a 所持	
		b 記憶	
設問 2	(1)	2	
		2	
		1	
		1	
	(2)	c 乱数を暗号化 又は ハッシュ値を生成	
設問 3	(1)	読み出せるようにすべき情報	5
		書き込めるようにすべき情報	6
	(2)	2	順不同
		3	
		4	
		5	
		7	
設問 4	(1)	項番 1	
		理由 失効 IC カードを一意に識別できるから	
	(2)	忘れた IC カードを運用管理者に提示するまでいったん失効する。	
設問 5	(1)	紛失した IC カードが不正使用され，スプールに滞留したデータが印刷される。	
	(2)	所定時間内に印刷されないデータは削除する。	

問 4

出題趣旨	
社外へ持ち出すことの多いノート PC や USB メモリからの情報漏えいを防ぐことの重要性が指摘されるようになって久しい。漏えい対策も様々なものが提案されている。 これらの対策を採用するに当たって重要なことは、情報の有効活用とのバランスをとることである。情報漏えいを防ぐためとはいえ、一律にノート PC の持出しや USB メモリの利用を禁止することは、企業活動の効率性や品質の確保という点からは、必ずしも適切な対策とはいえない。 本問では、現実の業務形態を考慮した上で情報漏えいのリスクを低減する対策を検討するという題材を通して、実務の中で有効な対策を考える能力を問う。	

設問	解答例・解答の要点		備考
設問 1	a	(イ)	
	b	(エ)	
	c	(コ)	
設問 2	復号のためのパスワードが、他者に推測されやすいものとなっている場合が多いから		
設問 3	(1)	スリープ状態からの復帰の際、パスワードを要求しないよう設定した場合	
	(2)	・スリープ状態から復帰すると、暗号化されたデータに第三者がアクセスできるから ・スリープ状態から復帰すれば、利用者がすべてのデータにアクセスできるから	
設問 4	e	Q	
	f	顧客に特別な環境を要求することなく暗号化したデータを渡せるから	
設問 5	(1)	・データ鍵とマスタ鍵が同時に流出する可能性が低いから ・NPC 上にデータを復号するために十分な情報がないから	
	(2)	・TPM は、鍵メモリに比べて総当たり攻撃に対する耐性が高く、パスワードの解析が困難であるから ・鍵メモリの場合、総当たり攻撃によってパスワードが解析され、マスタ鍵を読み出される可能性が高いから	
	(3)	d Q	