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 I 試験

問 1

出題趣旨
近年，ソフトウェアの脆弱性を悪用した攻撃について，脆弱性情報サイトなどからその攻撃手法が公開され対策が促される事例が増加している。 本問では，攻撃手法が公開されたソフトウェア脆弱性についての基礎知識及び与えられた条件の中でその影響範囲を考え対応策を検討する能力を問う。

設問		解答例・解答の要点			備考
設問 1		E システム	要素	可用性	
			理由	販売チャネルの大部分を担い，常時稼働が必要なため	
		F システム	要素	完全性	
			理由	投資家に正確な財務情報，会社情報を提供するため	
設問 2		a	公開ディレクトリ		
設問 3	(1)	b	ANY		b，d，f は，順不同
		c	遮断		
		d	COOKIE		
		e	遮断		
		f	Multipart		
		g	遮断		
	(2)	イ，ウ			
	(3)	h	エ		
	(4)	WAS を必要最小限の権限で動作させる。			
設問 4	①	・脆弱性 X を突く攻撃を防げること			
	②	・E システム利用のための正常な通信が許可されること			
設問 5		販売機会損失など，ビジネスへの影響を与えずに誤検知の検証ができる。			

問 2

出題趣旨
内部不正による情報漏えいを防止するためには，特権 ID の管理を含む委託先の管理が重要である。 本問では，特権 ID の管理を題材に，内部不正防止についての基本的知識を確認し，内部不正に対する課題を整理して対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問 1		a	Y 社の管理者	
設問 2	(1)	委託用特権 ID	DBMS 操作 ID	
		理由	業務アプリが DB サーバにアクセスする ID と同じ ID であるから	
	(2)	b	S 社 PC	
		c	管理用サーバ	
	(3)	不正操作の記録が管理用サーバの操作履歴に残るから		
設問 3	(1)	個人 ID が本人以外に使われるおそれがないように管理していること		
	(2)	抑止効果		
	(3)	委託先 PC にインストールするプログラムの資産管理をせずに済むから		

問３

出題趣旨
サイバー攻撃の増加に伴い，インシデント対応を適切に行える人材が必要となっている。 本問では，Web サイトへの侵入を想定し，侵入経路，原因及び影響範囲を調査，特定し，適切な対策を立案する能力を問う。

設問		解答例・解答の要点			備考
設問１		a	WebAP サーバ 2		
		b	WebAP サーバ 1		
		c	Web サーバ		
設問２	(1)	d	2		
		e	404		
		f	14		
		g	200		
	(2)	No.3 から 10 までのステータスコードが 401 で失敗を繰り返しており，No.11 は 200 でログインに成功しているから			
設問３	(1)	3，4			
	(2)	項番		5	
		サービス	①	・ファイル共有	
			②	・リモートデスクトップ	
設問４	(a)	サーブレットコンテナの管理画面に対するインターネットからの不正アクセス			
	(b)	自動的にログインを行う OS の仕様を利用した，他のサーバへの侵入			