平成 22 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
インターネットに公開されているサーバは，セキュリティ侵害の脅威にさらされている。サーバの導入時や更新時に，脅威への対応が行われていることを確認するため，セキュリティ検査の実施が望まれる。 本問では，システムの更新時に実施するセキュリティ検査を題材にして，ファイアウォール，SSH サーバ，DNS サーバ及びメールサーバに関する知識と設計能力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	SSH サーバの公開鍵が正しく，なりすましがないこと		
	(2)	**変更箇所**	(送信元) ・ あて先	
		変更後の内容	契約通信サービスにおいて割り当てられる Y 社専用の IP アドレス	
設問２	(1)	a	DNSSEC	
		b	ディジタル署名	
	(2)	アクセスしたい Web サーバとは別のサーバにアクセスしてしまう。		
	(3)	送信元ポート番号を固定する設定		
設問３	(1)	c	送信ドメイン認証	
	(2)	オ		
	(3)	d	受信者メールアドレスのドメイン名が y-sha.co.jp	
	(4)	メールサーバ 1 から送信される正常なメールが，ブラックリストを利用しているメールサーバで受信拒否される。		
設問４	(1)	非再帰的な問合せで，キャッシュ領域に保持されている Y 社管理ドメイン名以外の名前解決を行った場合		
	(2)	e	(a)	
	(3)	f	Y 社管理ドメイン名	
		g	DMZ	

問２

出題趣旨
これまでの情報セキュリティ対策では，予防策を中心とする事前の対策が重視されてきた。しかし，近年になってインシデント発生後の対応が適切か否かが組織の信頼や評判にも影響を及ぼすことが認識されるようになり，“事故前提社会”の観点からもインシデント対応に対する注目が高まりつつある。 本問では，ソフトウェア開発会社におけるインシデント対応体制の構築を題材として，インシデント対応についての理解や，インシデント対応に関連する種々の技術要素についての理解を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	プライバシーマーク	
		b	JPCERT	
	(2)	原因究明に必要な情報の収集に迅速かつ組織的に着手できること		
	(3)	出荷後の自社開発のソフトウェア製品に関するインシデント		
設問２	(1)	取得するログの種類や保管方法，保管期間		
	(2)	セキュリティに関する情報やソフトウェアの提供元の真正性		
設問３	(1)	c	アクセスがログに記録	
		d	ディレクトリトラバーサル	
		e	CONNECT	
	(2)	Web サーバがメールの不正中継に利用されるという問題		
	(3)	**理由**	対応が不要な警告メールが多いと対応が必要な警告メールを見落とすから	
		条件	DMZ では利用していないシステムや機能に関する警告メールであること	
設問４	(1)	再起動することでサーバ機上のファイルが改変される可能性があるから		
	(2)	解析の際に原本のデータを書き換えてしまう可能性があるから		
設問５	①	**問題**	開発系システムの構成情報が最新に保たれていなかったこと	
		記載内容	一時的な変更の際も，開発系システムの構成情報を常に最新に保つ。	
	②	**問題**	開発課の担当者が勝手にサーバ機をシャットダウンしたこと	
		記載内容	インシデント発生時の機器の操作は IRT の指示に従って行う。	