平成 23 年度　特別　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
電子メールは，コミュニケーションに有用かつ必須な手段となっている。しかし，メール誤送信による情報漏えいやウイルス感染の危険性がある。さらに，メーリングリストにおける同報機能によって危険性が高まり，情報セキュリティ対策が重要となる。 本問では，メールシステムの情報漏えい対策の強化を題材にして，電子メールに関する知識と設計能力及びメールシステムに関する情報セキュリティ対策の実施能力を問う。

設問		解答例・解答の要点		備考
設問１		a	ウ	
		b	ア	
		c	エ	
		d	イ	
設問２	(1)	送信者メールアドレスは，送信の許可と拒否の判定には使用しないから		
	(2)	**サーバの名称**	社内メールサーバ	
		確認した内容	S さんの PC の IP アドレスから，送信者メールアドレスが A さん用であるメールを送信したこと	
設問３	(1)	プロキシサーバ		
	(2)	社内メールサーバの POP3 スキャンを使用する。		
設問４	(1)	**見直し案**	社外メンバ登録 ML のドメイン名として，新たな P 社サブドメイン名を使用する。	
		設定ルール案	社外メンバ登録 ML のドメイン名を許可済ドメイン名に含めない。	
	(2)	① **項番**	2	①，②は順不同
		修正後の処理	社内メールサーバに転送	
		② **項番**	11	
		修正後の処理	社内メールサーバに転送	
	(3)	e	ML サーバ	
	(4)	メールからウイルスが広まった場合，メールを連絡手段として使えなくなるから		
	(5)	エンベロープの送信者メールアドレスに，ML アドレス管理者のメールアドレスを設定する。		
設問５	(1)	① ②	・アップロード時に，情報の取り違えに関する表示を行い，確認を促す機能 ・プロジェクトごと及び利用者ごとのアクセス権限を設定する機能 ・PJWeb サーバへの通信を暗号化する機能 ・アップロードされたドキュメントを一定時間の経過後に削除する機能	
	(2)	・プロジェクト終了後，削除申請されないと PJWeb サーバを不正に利用されるので，プロジェクト管理者に確認を行う。 ・PJWeb サーバのアクセスログを定期的に分析し，不正なアクセスの有無を確認する。		

問２

出題趣旨
組織体の情報資産に関わるリスクのマネジメントを効果的に実施する手法として，情報セキュリティ監査がある。情報セキュリティ監査人による独立かつ専門的な立場からの検証又は評価によって，組織体のマネジメントの向上を図ることが可能となる。 本問は，専門商社における情報セキュリティ監査を題材に，情報セキュリティ監査制度の知識，Web アプリケーション検査の技術，無線 LAN の強化，セキュリティ改善の手法などについて問う。

設問		解答例・解答の要点				備考
設問１	(1)	a	助言			
		b	保証			
		c	企業台帳			
	(2)	Y 社は K 社の開発委託先であり，監査の独立性を確保することが難しいから				
設問２	(1)	d	オ			
	(2)	リスクアセスメント				
	(3)	Z 社の IP アドレスからのスキャンは遮断の対象としない。				
設問３	(1)	e	クロスサイトスクリプティング			
		f	クロスサイトリクエストフォージェリ			
	(2)	g	セッションハイジャック			
設問４	(1)	h	802.1X			
	(2)	セッション管理用のクッキーに secure 属性を付与する。				
	(3)	・テスト時の実データの利用禁止 ・顧客情報の確実な返還，削除又は廃棄				
	(4)	**WPA-PSK では，**		一度情報を傍受された後は無線 AP に接続せず高速に試行を繰り返されてしまう	**のに対し，**	
		Web フォーム認証では，		攻撃を受けた場合，後続する試行を遅らせることができる	**から**	
設問５	(1)	**検出事項(1)**	・受発注 Web システムの改修に関する計画書 ・受発注 Web システムの受入れテストの結果			
		検出事項(3)	・無線 AP 及び HT の事前共有鍵変更に関する作業の記録 ・配送センタのシステム更改に関する計画書			
	(2)	・他社から求められたセキュリティ要件が K 社の管理策のレベルを超える場合，リスク分析を実施して他社と対応を協議する。 ・ある会社の営業秘密が，K 社を経由して他の会社に漏えいしないよう，秘密保持契約の内容を検討する。				