平成 24 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
本問では，広く利用されている Web のマッシュアップ技術に関する知識及び分析力を問う。特に，Same-Origin ポリシの概念及びクロスドメインでのデータ取得の仕組みに関する理解力を問う。

設問		解答例・解答の要点		備考
設問 1		a	エ	
		b	ウ	
設問 2		利用者がクライアント証明書を用意する必要がない。		
設問 3	(1)	c	会員サイト	
		e	ブラウザ	
	(2)	悪意ある JSONP 呼出しスクリプトを実行するブラウザが，会員サイトにログインした状態である場合		
	(3)	d	JSONP 型データ	
設問 4	(1)	f	認証された利用者	
	(2)	g	送信されない	

問 2

出題趣旨
ログのモニタリングは，システムにアクセスする権限をもった利用者による不正を検出する仕組みとして有効である。しかし，適切なモニタリング条件が設定されないと，不審な行動を見逃してしまったり，逆に，通常業務としての利用が大量に検出されてしまったりするなど，期待どおりには機能しない。 本問では，システムの利用状況を基に，適切なモニタリング条件を設定する能力及び，モニタリングを有効に維持し続けるプロセスを確立する能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	個人情報へのアクセス頻度の上限のような具体的な値		
	(2)	a	8000 番台の機能の利用失敗回数が 1 回以上	
	(3)	ログイン失敗		
設問 2	(1)	悪意ある行動を抑止する効果		
	(2)	モニタリング条件を回避するようにして悪意ある行動をとられること		
	(3)	新サービス担当の 4 名以外の従業員が 1 週間で 50 回を超えて 200 回以下の頻度で個人情報へのアクセスを行った場合		
	(4)	b	1 週間で，8000 番台の機能の利用成功が 50 回を超え	
設問 3		定期的に営業部の部長にヒアリングを行って業務内容に変化がないか確認し，モニタリング条件を見直す。		

問３

出題趣旨
標的型攻撃は，従来のセキュリティ対策の隙をつく攻撃で，対策が容易ではない。本問では標的型攻撃の実例を示す中で，インシデント分析技術と出口対策というトータル対策の立案能力を問う。また電子メールの信頼性を確認できる送信ドメイン認証を話題として取り上げ，その導入に関する技術知識を問う。

設問		解答例・解答の要点		備考
設問１		a	ウ	
		b	ア	
設問２	(1)	c	オ	
		d	イ	
	(2)	e	z.y.x.1	
設問３	(1)	メール中の社外サイトのリンクをたどった		
	(2)	**システムの名称**	ネットワークモニタ	
		設置場所	社内 LAN 上	
		監視すべき事象	トラフィックの急激な増加	
	(3)	FW は PRX と MX1 からだけインターネットとの通信を許可している。		
	(4)	通信先が信用できるかをシグネチャで判断する Web フィルタを PRX に導入する。		

問４

出題趣旨
インシデント対応については，様々なログからインシデント発生の検知と内容の把握をし，インシデントを封じ込めるための対策，根本原因の把握と解決，フィードバックからの運用強化が重要になる。本問では，その一連のプロセスを正確に理解し，事態に対処できる能力を問う。

設問		解答例・解答の要点		備考
設問１		CPU の使用率を確認することで，普段と異なる事象が発生している時間帯が見極めやすくなるから		
設問２	(1)	a	△△.123.123.123	
	(2)	表 5(3)，表 6(1)		
	(3)	該当通信は，Web サーバのステータスコードが 200 であるから		
設問３	(1)	b	送信元 IP アドレス	
		c	・https ・SSL	
		d	秘密鍵	
	(2)	Web サーバプログラムで制限している最大同時セッション数の不足		
	(3)	**機器①**	ウ	機器①，設定内容①と機器②，設定内容②は順不同
		設定内容①	X-Forwarded-For ヘッダフィールドの追加	
		機器②	オ	
		設定内容②	X-Forwarded-For ヘッダフィールドのアクセスログへの出力	