平成 24 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 I 試験

問 1

出題趣旨
Web アプリケーションの脆弱性検査の指摘事項に対する正しい対応策を問う。エスケープ処理では，出力する文脈に合わせた処理を行う必要がある。 本問では，特に，スクリプトを動的に生成する場合のセキュアプログラミングに関する知識を問う。

設問		解答例・解答の要点			備考
設問１		a	secure		
		b	GET		
設問２	(1)	端末の IP アドレスがセッションの途中で変わるようなアクセスの場合			
	(2)	攻撃者と被害者が同一のプロキシサーバや NAT を経由してアクセスした場合			
	(3)	クエリ文字列にスクリプトが含まれているログを検出する。			
設問３	(1)	c	37		
	(2)	①	d	\（バックスラッシュ）	①と②は順不同
			e	\\（バックスラッシュ＋バックスラッシュ）	
		②	f	’（シングルクォート）	
			g	\’（バックスラッシュ＋シングルクォート）	

問 2

出題趣旨
Web システムに対する攻撃は非常に多いにもかかわらず，インシデントが発生した後のサーバ管理者又は運用者の対応は必ずしも万全とはいえない。 本問では，Web サーバのアクセスログを見て何が起きたのかを理解し，そのインシデントに関する適切な対応とセキュリティ対策を問題として取り上げた。

設問		解答例・解答の要点			備考
設問１	(1)	a	ipH		
	(2)	b	search		
	(3)	特徴	同一 IP アドレスから，	一つの会員 ID に対して様々なパスワードでログインを試みている。	
		対策	連続してログインに失敗した時は，その会員 ID をロックする。		
設問２	(1)	d	コ		
		e	エ		
		f	ウ		
		g	ク		
	(2)	他のサイトで同じ会員 ID，パスワードを使用している会員に対し，その変更を促す必要があるから			
設問３	(1)	c	プラグイン		
	(2)	偽の入力画面を表示させ，そこに入力させた情報を攻撃者が用意したサイトに送信する。			

問３

出題趣旨
近年，機密情報の漏えい時の調査や外部監査対応時の証跡提示などの目的から，IT システムの利用者のアクセスログだけでなく，操作内容を記録する企業が増えてきている。操作内容を記録する場合，その目的や対象利用者のアクセス権などを考慮しなければ，記録した内容の真正性に疑義が生じる可能性がある。 本問では，業務委託先作業担当者の操作内容の証跡確保を題材として，セキュリティ上の考慮点を問う。

設問		解答例・解答の要点		備考
設問１	(1)	b	改ざん検知	
	(2)	ウ		
設問２	(1)	a	エージェントモジュール	
	(2)	c	Z 社 PC	
		d	中継サーバ	
設問３	(1)	保険サーバに一時保管された操作ログを削除する操作		
	(2)	エージェントモジュールを停止させる操作		
	(3)	エージェントモジュールを停止させる操作を検知ルールに設定する。		
設問４	(1)	Z 社の保守チームに，操作ログを取得し，監視していることを伝える。		
	(2)	作業計画書に記載された作業担当者と一致する利用者 ID にだけ，中継サーバから保険サーバへのアクセスを許可する。		

問４

出題趣旨
セキュリティ技術者が不足していると言われているものの，その育成については個々の現場に委ねられている状況が見受けられる。しかし，セキュリティ技術者の育成に当たっては演習などを通じた実践的な育成が重要である。 本問では，標的型攻撃という題材を取り上げつつ，現実に近いネットワーク環境での演習による技術者の育成について問う。

設問	解答例・解答の要点		備考
設問１	下線①	メール受信者に正常なメールと誤認識させて添付ファイルを開かせるため	
	下線②	ウイルス対策ソフトで検出されることを防ぐため	
設問２	不正な通信の送信元 TCP ポート番号を基に，そのポートを使用しているプログラムを特定する。		
設問３	正常な OS で起動した他の PC に，複製した PC のハードディスクを接続してファイルを取り出す。		
設問４	添付ファイルの安全が確信できない場合，電話などで送信者に送信の事実を確認する。		