平成 23 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
Web アプリケーションの脆弱性対策の基本的な考え方は，プログラム言語にかかわらず共通であると言える。しかしながら，セキュアなプログラミングを実践するためには，使用している言語の特性を理解した上でその特性に合った対応をとる必要がある。 本問では，二つのプログラム言語の比較を通して，それぞれのプログラム言語の特性に合った脆弱性対策を正しく認識しているかを問う。

設問		解答例・解答の要点		備考
設問 1	(1)	user, day		
	(2)	a	プレースホルダ	
	(3)	b	prepareStatement	
	(4)	ア		
	(5)	c	HTML における特別な記号	
		d	エスケープ	
	(6)	user, day, rep		
設問 2		e	ポインタ	
		f	バッファオーバフロー	
		g	ガーベジコレクション	
設問 3		アドレスを計算対象にできないから		

問 2

出題趣旨
システムに対して，現行の設計を十分に考慮せず不用意に機能を追加することで，セキュリティ上の問題が発生する事例は少なくない。 本問では，システムへの機能追加に関する開発プロジェクトの設計工程において，セキュリティの観点でのレビューを適切に実施することで問題点を指摘し，適切な修正案を提示する能力を問う。

設問		解答例・解答の要点		備考
設問 1		a	エ	
設問 2		b	status の値が 0	
		c	lockout_t の値から 60 分以上経過している	
		d	fails の値が 4 以下	
		e	temppass の値が 0	
設問 3	(1)	サスペンド状態の UID に対するパスワード初期化によって利用者がサスペンドを解除できる。		
	(2)	status の値が 2 の UID はパスワード初期化を実行しない。		
設問 4		仮パスワードを知っているのが利用者だけであるから		
設問 5		取得ページ URL を通知するメールを盗聴し，利用者より先に取得ページにアクセスする手口		

問３

出題趣旨
クラウドサービスの発展によって，企業におけるインターネット上の Web サービスの利用が増加傾向にある。Web サービスには SSL を用いることが多いが，プロキシで Web アクセス時のログを取得する場合，通信内容が暗号化されているので詳細なログを取得できない。 本問では，HTTPS 通信時におけるプロキシでのログ取得を題材として，HTTPS 通信時の動作及び証明書の検証についての理解を確認する。

設問		解答例・解答の要点		備考
設問１	(1)	ログを平文で記録できないから		
	(2)	(2)，(3)，(5)		
	(3)	ア		
設問２	(1)	a	中間者	
	(2)	① ②	・サーバ証明書のコモンネームとアクセス先のホスト名が一致すること ・サーバ証明書がブラウザで信頼する認証局から発行されていること	
設問３	(1)	b	L プロキシのルート証明書を信頼するルート証明書としてインストールする	
	(2)	証明書 2 はブラウザが信頼する認証局が発行したものではないから		
	(3)	サーバ証明書のコモンネームとアクセス先のホスト名を一致させるため		

問４

出題趣旨
財務報告の信頼性確保を目的に内部統制報告書作成が義務付けられ，その中で情報セキュリティを扱う場面も多くなってきている。 本問では，内部統制を題材に，JIS Q 27002 による情報セキュリティマネジメントの基本知識を確認し，更に情報セキュリティ確保のために技術的及び管理的視点から必要な情報セキュリティに関するマネジメント能力を問う。また，最近では，クラウドサービスや ASP サービスのような外部サービスの利用が増加しており，外部サービス利用時における情報セキュリティの確保に対して必要な知識を問う。

設問		解答例・解答の要点		備考
設問１		a	アクセス制御	
設問２		b	クリアデスク	
		c	認証トークン	
		d	スクリーンロック機構	
		e	プリンタから速やかに取り出して	
設問３	(1)	ウ		
	(2)	鍵付きハッシュ値などによる改ざん検知対策		
	(3)	USB メモリに関わる作業の複数人化による相互けん制		
設問４	(1)	f	第三者	
	(2)	Q 社から依頼された利用者 ID の登録に関する承認手続		