平成 22 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
情報システムの障害において，原因分析のために取得される資料データには，ユーザ企業の秘密情報が含まれることがあり，その取扱いには十分なセキュリティ確保に対する配慮が必要である。 情報システムの障害の発生頻度は低い反面，障害発生時には迅速な対応が求められることから，資料データの伝送には費用が安く，高速なインターネットの利用がしばしば求められる。 本問は，大企業のマルチベンダシステムにおける資料データの伝送方式のセキュリティ設計を題材として，費用とのバランスを考慮しながら必要十分なセキュリティを設計する能力と実務経験を問う。

設問		解答例・解答の要点		備考
設問 1		a	なりすまし	
		b	クライアント証明書	
		c	盗聴	
設問 2	(1)	Web サーバが SI ベンダ間で共用されるから		
	(2)	**アクセス対象**	各 SI ベンダ専用のディレクトリ	
		アクセス元の利用者	ほかの SI ベンダの保守担当者	
設問 3	(1)	① ②	・通信ログ ・作業報告書	
	(2)	運用担当者と保守担当者それぞれの個人に異なる利用者 ID を割り当てておく。		
	(3)	① ② ③	・日時 ・利用者 ID ・ファイル名	
設問 4		各 SI ベンダが所有するベンダ PC への設定が必要だから		

問 2

出題趣旨
利用されるシステムが増えるとともに，ID の管理コストの増大やセキュリティ確保の困難さが指摘されるようになり，ID の統合に取り組む事例が増えている。 本問では，ID の統合を検討するのに不可欠な，ID の管理方法についての基本的知識を確認し，組織の状況を判断して運用設計を行う能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	a	無効	
		b	有効	
	(2)	c	不許可	
		d	パスワードを設定してください。	
	(3)	e	24 時間を超えた	
設問 2	(1)	UID 削除予定日　又は　契約満了予定日　又は　アカウント終了予定日		
	(2)	4		
	(3)	契約管理部が，契約解除を確認し，UID 削除依頼を行う。		
設問 3		他人の UID のパスワードを 5 回連続して間違え一時利用停止状態とし，アカウント管理者にパスワード初期化を依頼する場合		
設問 4		・パスワード初期化依頼の際には，上司からメールで依頼する。 ・仮パスワードの連絡は，あらかじめ登録された電話番号だけに限定する。		

問３

出題趣旨
Web アプリケーションに脆弱性が発見された場合に，Web サイトが置かれた環境やその他の諸事情によって，脆弱性の修正作業が長期化する事例が少なくない。 本問では，脆弱性を悪用した攻撃から Web アプリケーションを保護するための Web アプリケーションファイアウォール（WAF）の導入を題材として，WAF が有効な状況，WAF の機能，WAF の導入における留意点などの理解を問う。

設問		解答例・解答の要点	備考
設問１		a　エ	
設問２		FW はパケットのヘッダ情報だけでアクセスを制御するから	
設問３	(1)	復号後に有効なセッション ID となる暗号文を攻撃者が生成できないから	
	(2)	ウ	
	(3)	・クッキーがクライアント上で参照される場合 ・クッキーが WAF を経由しない別の Web サーバへ送信される場合	
	(4)	無効化するシグネチャで定義された攻撃の対象となる脆弱性が，Web アプリケーションやミドルウェアに存在しないこと	
設問４		利用者のブラウザと Web サーバ間で通信が SSL 暗号化されていると，WAF が攻撃の検知をできないから	

問４

出題趣旨
昨今のマルウェアを利用した攻撃は複合的になっており，PC，サーバの両方で様々な対策を実施する必要がある。その総合的な知識を問う。また，攻撃を受けた後，再発防止に当たって，業務への影響を考えた上での短期的な対策と，今後の攻撃の変化に備えた長期的な対策を，メリハリをつけて実施する実務的な対処・遂行能力を問う。

設問			解答例・解答の要点	備考
設問１		a	セキュリティパッチ	
		b	ブラック	
		c	脆弱	
設問２	(1)	ア	(4)	
		イ	(2)	
		ウ	(1)	
		エ	(3)	順不同
		オ	(4)	
	(2)		プロキシサーバ	
設問３	(1)	① ②	・共用 PC から FTP アクセスした本番サーバ及びテストサーバを調べる。 ・本番サーバ及びテストサーバでの改ざんがないかの調査を依頼する。	
	(2)		不正プログラム送り込みサイトが業務で利用する Web サイトであり，URL フィルタでは遮断されない場合	