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Ⅰ試験

問１

出題趣旨
堅ろうなプログラムを開発するためにはバッファオーバフロー脆弱性を作り込まないことが重要なポイントである。 本問では，バッファオーバフロー脆弱性の理解と，その対策について問う。特に対策については，脆弱性の発見と修正だけでなく，そもそも脆弱性を作り込まないための仕組みまで踏み込める能力を問う。

設問		解答例・解答の要点		備考
設問１		a	ア	
		b	ウ	
設問２	(1)	dst が指し示す領域		
	(2)	dst が指し示す領域の残りが 2 バイト以下となった時点で，src にエンコードすべき文字があった場合		
設問３		c	文字列を string クラスとして取り扱っており，領域の境界は処理系が管理することとなる	
設問４		d	文字型の配列	
		e	上限チェック	
		f	代入	

問２

出題趣旨
ソフトウェアライセンスに対する違反行為が，最近，社会問題になっている。 本問では，管理ツールによるソフトウェアの実態把握を通じて，ソフトウェアライセンス，セキュリティパッチ，運用管理に関する知識と対応能力を問う。

設問		解答例・解答の要点	備考
設問１	a	アップグレード	
	b	損害賠償	
	c	著作権	
設問２		遊休ライセンスを全社で有効利用する可能性	
設問３		インストール情報が存在しなくても，実行情報は存在するから	
設問４	(1)	インストール情報に，特定のセキュリティパッチが含まれていない PC を抽出する。	
	(2)	脆弱性が発見されても対処する手段がない，という状況を回避することができる。	
	(3)	異動に伴い不要になったソフトウェアを削除する。	
設問５		ライセンスの利用者と登録者の間で相互けん制が働くから	

問３

出題趣旨
情報セキュリティ対策の立案に当たっては，情報資産の利用状況から想定されるリスクへの対応の有効性確保という観点が必要である。利用状況からは想定されないリスクにだけ対応した対策や，想定されるリスクに対して無効な対策を立案するようなことは避けなければならない。 本問では，情報（情報を保存した機器や媒体）の持出しという題材を通して，リスクを考慮して情報セキュリティ対策を立案する能力を問う。

設問		解答例・解答の要点	備考
設問１	(1)	暗号化	
	(2)	イ	
設問２		移動中は肌身離さず持つ。	
設問３	(1)	当該持出時に必要な情報以外に貸与 PC に入っている業務情報も漏えいする可能性があるから	
	(2)	顧客を訪問する直前に業務情報をアップロードし，ダウンロードされたらすぐに削除する。	
	(3)	アップロードする業務情報が，当該顧客向けの情報であること	
設問４		セキュリティ対策が十分でない可能性のある私有 PC に業務情報をダウンロードすることができてしまうから	

問４

出題趣旨
インターネットに公開する Web システムでは，セッション管理の不備，クロスサイトスクリプティング，SQL インジェクションなどのアプリケーションの脆弱性に加え，アカウント窃取やコンテンツ管理業者による内部不正についての対策も欠かせない。 本問では，インターネットに公開する Web システムにありがちな脆弱性と攻撃手法という題材を通して，これらへのセキュリティ対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	ウ	
	(2)	scp　又は　sftp		
	(3)	b	公開鍵認証方式	
	(4)	定期的に FW のドロップログを分析し，拒否した通信から調べる。		
	(5)	**閲覧するための方法**	DB に接続して会員データを復号し表示するスクリプトファイルを作成し，実行して閲覧する。	
		暫定対策の内容	CNT-MGR から全てのスクリプトファイルへのアクセス権限を削除する。	
設問２		一定時間内に同一 IP アドレスから複数の会員 ID でログイン試行し，かつ，一定回数以上認証失敗していること		