平成 28 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 II 試験

問 1

出題趣旨
パスワードを用いた利用者認証の仕組みには限界があり，IC カードや OTP トークン，携帯電話を用いた利用者認証の仕組みがますます重要になってきた。これらの仕組みにおいては，公開鍵暗号技術をはじめとする各種の暗号技術，認証技術が幅広く採用され，利用されている。 本問では，利用者認証システムの構築を題材に，IC カード，PKI，暗号及び認証についての基礎的知識と，これらの技術を利用したシステムの構築及び運用についての設計能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	ウ	
		b	オ	
		c	ス	
		k	エ	
		l	イ	
	(2)	認証対象者が，認証カードと PIN を他人に又貸しして使わせる行為		
	(3)	d	ウ	
		e	カ	
		f	ク	
	(4)	ア，イ，エ，キ，ク，ケ		
	(5)	g	イ	
		h	オ	
		i	ア	
		j	セ	
設問２	(1)	① ②	・申請者に認証カードを貸与済みでないこと ・申請者が事業用システムの利用を業務上必要としていること	
	(2)	ア		
	(3)	改善すべき不備	失効の申請がされてから失効情報の開示まで最短でも 2 日掛かるという不備	
		失効事由の値	ア，ウ	
設問３	(1)	サーバ証明書の正当性を確認できず警告が表示される。		
	(2)	PC の Web ブラウザが不正なサーバ証明書を信頼し，不正なサーバにアクセスするリスク		
設問４	(1)	認証を成功させても，事業用システムの利用の認可が得られないから		
	(2)	① ②	・事業部門は管理責任者の役割を担わず，認証カードの配布・回収を担当しないから ・プロジェクトをまたいで認証カードが共用され，配布・回収の回数が少ないから	
	(3)	入退室に必要なため，認証カードの置き忘れ及び現場事務所内での保管がなくなる。		

問２

出題趣旨
本問は，情報システムを運用する組織における脆弱性対応に関する問題である。昨今，広く利用されている機器において重大な脆弱性が連続的に報告されることがあり，機器を利用する側としては，緊急性を要する脆弱性にどのように対処するのかが問われるケースが増えてきた。個別の脆弱性に場当たり的に対処するのでは非効率であり，脆弱性対応を行う作業者の負荷も考慮し，迅速かつ的確に脆弱性に対応する必要性が増している。 本問では，脆弱性が及ぼす影響を技術的に判断する能力，及び頻発する脆弱性への組織的対応方法に関する知識を問う。

設問		解答例・解答の要点		備考
設問１	(1)	ウ		
	(2)	脆弱性が発見された特定のバージョンのソフトウェアが導入された機器を迅速に特定するため		
設問２	(1)	ウ		
	(2)	ウ		
	(3)	a	HTTP リクエスト	
	(4)	`() { echo test; }; /usr/bin/cat /etc/passwd`		
設問３	(1)	b	パターンマッチング	
	(2)	WAF の場合，検証作業の試験項目がパッチ適用のときよりも少なくて済むから		
	(3)	c	ウ	
		d	イ	
	(4)	通信量の上限の切替えで WAF の能力変更が随時可能，かつ作業工数やコストの観点から無駄がない。		
設問４	(1)	f	社内 Web サーバの URL	
	(2)	e	オ	
		g	ア	
		h	キ	
	(3)	プロキシサーバを通じて攻撃者のサイトと通信する機能		
設問５	(1)	i	中	
	(2)	ア，ク		
	(3)	j	重要情報が漏えいする	順不同
		k	社外から侵入される	