令和３年度　春期　情報処理安全確保支援士試験　解答例

午後 II 試験

問 1

出題趣旨
昨今，サイバー攻撃が高度化してきており，その中で様々な情報セキュリティインシデントを防ぎ，かつ，迅速に処理するためにも，情報セキュリティについてより一層広範な知識と技術，運用の知見が求められるようになってきている。 本問では，インシデント対応体制の整備を題材に，インシデント対応のための仕組みの設計及び運用に関する能力，並びにアクセス制御，脆弱性管理などインシデントを防ぐための知識及び技術力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	外部から入手した利用者 ID とパスワードの組みのリストを使ってログインを試行する攻撃		
	(2)	他のサービスで利用したパスワードとは別のものを設定すること		
	(3)	・IP アドレスから分かる地理的位置について，過去のログインのものとの違いを確認する。 ・Web ブラウザの Cookie を利用し，過去にログインした端末かを判定する。		
	(4)	a	タイムゾーン	
	(5)	b	9	
設問２		マルウェアに感染した USB メモリを介して管理用 PC に侵入し，さらに店舗管理サーバへ侵入する。		
設問３	(1)	c	オ	
	(2)	d	イ	順不同
		e	カ	
		f	ウ	
設問４	(1)	5		
	(2)	脆弱性 M を悪用しても一般利用者権限での操作であるが，“/etc/shadow”ファイルの閲覧には管理者権限が必要であるから		
	(3)	攻撃の接続元 IP アドレスを“/etc/hosts.allow”ファイルに追加する。		
	(4)	24		
	(5)	FW2 において，インターネットからのインバウンド通信は N 社と V 社からの通信だけを許可する。		
設問５		・複数の脆弱性が同時に悪用される可能性の観点 ・対応を見送った脆弱性の影響の観点		

問２

出題趣旨
クラウドサービスの活用は利便性の向上やコストの利点があり，昨今，IT の潮流になっている。クラウドサービスの活用に対し慎重な判断をする企業もある一方で，新興企業では，急速にクラウドサービスへ移行しつつある。クラウドサービス利用においては，外部の専門家からの支援を受けながら IT 統制を構築し運用することが行われている。 本問では，クラウドセキュリティを題材に，利用部門がクラウドサービスを利用していく上で，IT 部門として必要となる技術力及び判断力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	オ		
	(2)	多くの個人所有機器を C 社内 LAN に接続することによって，IP アドレスが枯渇するという問題が引き起こされた。		
	(3)	稼働させたまま行う方法	L2SW にミラーポートを設定し，そのポートに LAN モニタを接続して DHCP OFFER の数を確認する。	
		停止させて行う方法	DHCP による IP アドレスの配布がないことを確認する。	
設問２		企画部の部員がアクセスできるチャットエリアで共有されている情報		
設問３	(1)	a	C-PC	
		b	AP	
	(2)	c	エ	
設問４	(1)	・インターネットを使って情報収集する業務 ・事業部や企画部の顧客への提案や企画の立案		
	(2)	2		
	(3)	1		
	(4)	記号	ウ	
		方法	TLS クライアント認証による検証	
設問５	(1)	・ISAE3402/SSAE16 ・ISMS 認証		
	(2)	d	4	
設問６	(1)	秘密鍵を書き出しできないように設定する。		
	(2)	管理者が，P ソフトを，一般利用者権限では変更できないように設定する。		