令和元年度　秋期　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
本問では，Web アプリを開発し運用する現場における，セキュリティインシデント対応及びセキュリティ対策についての能力を問う。また，従来型のウォーターフォール型の開発ではなく，いわゆる DevOps を実践する企業における対応力を問う問題である。高度化する開発及び運用においては，営業的に求められる機能の開発だけに注力するのではなく，DevOps に伴うリスクを認知し，それらへ対処することが必要となるので，その能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	DBMS-R における同じ脆弱性を悪用されて，別のマルウェア X またはほかのマルウェアに再度感染してしまい，マルウェア X の動作が阻害される。		
	(2)	α	カ	
		β	ク	
		γ	ア	
	(3)	マルウェア X には，暗号資産の採掘プログラムによる採掘演算結果以外の情報を外部に送信する機能はなく，マルウェア X 以外による遠隔コマンド実行及び SSH サービスへの接続がなかったから		
設問 2	(1)	対策 1	（イ）	
		対策 2	（イ）	
		対策 3	（ア），（エ）	
		対策 4	（ウ），（エ），（オ）	
	(2)	あ	22/tcp	
		い	6379/tcp	
		う	a2.b2.c2.d2	
	(3)	a	curl	
		b	iptables	
	(4)	え	オ	
		お	カ	
		か	キ	
設問 3	(1)	ア，ウ		
	(2)	S 社のシステムを構成する実行環境のバージョン情報を把握して，その情報を常に最新にしておくこと		
	(3)	き	ア	
		く	ウ	
	(4)	け	レビュー	
		こ	第三者	
設問 4		c	オ	
		d	ア	
		e	エ	
		f	カ	
		g	キ	
		h	ウ	

問２

出題趣旨
産業用制御システムなどの OT のシステムと IT のシステムは分離すべきと言われている。しかし，実際には，中規模，又は大規模な工場であっても，OT 用と IT 用のネットワークが分離されていないケースが多く見られる。 本問では，OT と IT が混在する環境の課題を示し，それぞれの目的を念頭に置きながら，課題解決のための案を検討する。インシデント対応，APT 攻撃の概念モデル，ネットワーク分離，無線アクセス認証，セキュリティ規程など，幅広い分野についての実践的な知識と，目的・条件に合わせて様々な技術を組み合わせ，課題を解決する能力を問う。

設問		解答例・解答の要点			備考
設問１	(1)	User-Agent ヘッダフィールドの値が A 社で利用している Web ブラウザを示す値であるケース			
	(2)	a	エ		
	(3)	b	ア		
	(4)	c	サイト U		
設問２	(1)	d	カ		
		e	キ		
		f	オ		
	(2)	活動 1	1		
		活動 2	7		
		活動 3	3		
設問３		g	電波を傍受		
		h	MAC アドレス		
設問４	(1)	攻撃者の操作指示が FA 端末に伝えられない。			
	(2)	i	イ		
		j	ウ		
		k	ア		
	(3)	USB メモリをマルウェア対策ソフトでスキャンする。			
設問５	(1)	事務 LAN 用	（い）		
		センサ NET 用	（か）		
	(2)	事務 LAN とセンサ NET は F-NET と分離されており，AP に不正接続しても FA 端末を攻撃できないから			
設問６	(1)	イ			
	(2)	①	・当該脆弱性に対応したパッチを適用する。		
		②	・脆弱(ぜい)性をもつソフトウェアの利用を停止する。		
設問７	(1)	図 4	工場 LAN	エ	
			標準 PC	エ	
			FA 端末	ア	
		図 5	事務 LAN	エ	
			F-NET	ア	
			センサ NET	ア	
			標準 PC	エ	
			FA 端末	ア	
	(2)	①	・各部門が定めた管理・維持のための措置		
		②	・リスクアセスメントの結果		