平成 30 年度　春期　情報処理安全確保支援士試験　解答例

午後 I 試験

問 1

出題趣旨
ヒープ領域に関連する脆弱性は，特定の手順でメモリ操作を行った場合だけ発現するものが多いことから，発見しづらく，スタック領域に関連する脆弱性よりも対策漏れが起きやすい。近年では，Web ブラウザ製品などで特に多く発見されており，ドライブ・バイ・ダウンロード攻撃に悪用されるものも多い。 本問では，Use-After-Free 脆弱性を題材に，メモリ上の任意のアドレスに攻撃コードが書き込まれて実行される仕組みを理解し，脆弱性対策が適切に実装されているかを評価する能力を問う。

設問	解答例・解答の要点		備考
設問 1	a	カ	
	b	ウ	
設問 2	785634120a		
設問 3	c	（エ）	
設問 4	d	0x0b123400	
設問 5	e	ヒープ	
設問 6	ライブラリ関数はデータ実行防止の対象ではないメモリ領域に配置されているから		
設問 7	f	（ア）	
設問 8	g	DisplayNote	
設問 9	h	m_note = NULL;	

問 2

出題趣旨
サーバの運用管理に利用する PC は，特権 ID を用いたサーバへのログインに用いられることが多い。そのため，当該 PC にログインできるアカウント情報が窃取されると重大な被害につながることから，一般の業務に利用される PC より強固な情報セキュリティ対策が求められる。 本問では，サーバの情報セキュリティ対策強化を題材に，運用管理に利用する PC，ネットワーク及びサーバの情報セキュリティ対策に関する設計能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	a	x1.y1.z1.4	
	(2)	b	迷惑メール対策サーバ	
		c	Web メールサーバ	
		d	外部メールサーバ	
設問 2	(1)	e	インターネット上のドメイン名についての名前解決	
	(2)	① ②	・インターネットへのメールの送信を許可されていない従業員が，送信できるという問題 ・送信者メールアドレスを詐称したメールを送信できるという問題 ・マルウェアのスキャンを行わずにメールを送信できるという問題	
設問 3	(1)	運用 PC からの接続も拒否するように変更する。		
	(2)	運用 PC から接続できる URL は，T 社標準ソフトのベンダのサイトのものだけに制限するように変更する。		

問３

出題趣旨
情報システムのセキュリティ対策として，ネットワーク分離の仕組みを導入する例が増えている。しかし，ファイル転送や脆弱性対策，マルウェア対策などのために何らかの接続が必要である場合が多い。ここで接続の仕組みが不適切であると有効なセキュリティ対策にならないおそれがある。 本問では，創薬ベンチャ企業のネットワーク分離を題材に，機密性の高い情報を保護しながらも，分離したネットワーク間で安全にファイル転送ができる仕組みを設計する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	ウ	
		b	エ	
	(2)	c	ア	順不同
		d	ウ	
設問２	(1)	ファイル転送サーバから研究開発 PC への通信は FW2 で禁止されているから		
	(2)	e	利用者 ID	順不同
		f	パスワード	
		g	アップロード用 URL	
		方法	事務 PC の HTTP リクエストを監視する。	
	(3)	研究開発 PC からファイル転送サーバにアクセスして，ファイルをダウンロードする必要があるから		
設問３		h	高い	
		i	通信経路上に感染活動を遮断する機器が存在しないから	
		j	低い	
		k	FW2 によって感染活動を遮断できるから	
設問４		l	上長による承認	