平成 30 年度　秋期　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
昨今，多くのアプリケーションで様々な脆弱性情報が報告されるが，開発者のみならず，ユーザ企業のセキュリティ担当者（CSIRT のテクニカル担当）もそのリスクの程度を正確に推定できることが必要であると考える。 本問では，ソフトウェア開発における脆弱性の対策技術について問う。特に，バッファオーバフロー脆弱性（メモリ破壊脆弱性）について，ユーザ企業のセキュリティ担当者がその仕組み及びその対策について知っておくべき内容を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	a	キ	
		b	カ	
		c	ウ	
		d	ア	
	(2)	あ	㋒	
	(3)	shell コードが DEP で実行禁止にされているスタック領域にあるから		
設問 2	(1)	e	canary	
		f	ASLR	
	(2)	g	strcpy	
設問 3	(1)	行番号	16 行目	
		排除できない理由	ポインタを使って直接メモリ操作しているから	
	(2)	問題	メモリ破壊攻撃を防げないこと	
		開発環境	SSP を適用できないコンパイラを利用する開発環境	

問 2

出題趣旨
2017 年に WannaCry ワームによる世界規模でのシステム障害が発生した。ネットワークワームによる大規模な被害は，2008 年の Conficker ワーム以来であり，短時間でネットワーク内の多数の端末に感染するようなワームに対し，迅速に対応できる人材の必要性が再認識された。 本問では，自律的に自らの複製を拡散させ感染を拡大するという特徴をもつマルウェアへの感染を題材に，ネットワークの状態を把握し，インシデント発生時には迅速に対応できる能力を問う。

設問		解答例・解答の要点		備考
設問 1		a	ウ	
		b	ス	
		c	セ	
		d	エ	
		e	コ	
設問 2	(1)	SYN+ACK		
	(2)	(a)	パケットが NSM センサの監視対象外であるため	
		(b)	同一 IP アドレスへのスキャン回数は少ないから	
設問 3	(1)	PC101，PC133，PC277，PC301，PC321，PC340		
	(2)	イ，オ，カ		
設問 4	(1)	①	・セキュリティ修正プログラムが適用されていること	
		②	・マルウェア定義ファイルが更新されていること ・PC がマルウェアに感染していないこと	
	(2)	VLAN を使い，PC 間の通信を禁止する。		

問３

出題趣旨
インターネット公開サイトにおいて，OS やミドルウェアの脆弱性を突いた攻撃が頻発しており，情報漏えいなど，甚大な被害を受ける例が後を絶たない。それに対して，セキュリティ担当者は，業務継続を意識した対策を見出すことが求められている。 本問では，アプリケーションフレームワークについてのインシデント対応と WAF の導入を題材に脆弱性を悪用する攻撃に対する対応と，与えられた条件下でセキュリティ上の課題を特定し改善する能力を問う。

設問		解答例・解答の要点		備考
設問１		NTP による時刻同期		
設問２		a	CVSS	
設問３		E サーバをネットワークから切り離して，待機サーバを公開する。		
設問４	①	調査すべき機器	外部メールサーバ又はログ管理サーバ	
		調査すべき内容	外部メールサーバからサイト Z への接続の有無を確認する。	①，②又は③の組合せとする。
	②	調査すべき機器	E サーバ又はログ管理サーバ	
		調査すべき内容	外部メールサーバへの SSH コマンドの接続の有無を確認する。	
	③	調査すべき機器	FW1 又はログ管理サーバ	
		調査すべき内容	サイト Z と HTTP を使用した通信を確認する。	
設問５	(1)	b	攻撃	
	(2)	インターネットからの HTTPS 通信を復号する機能		
	(3)	c	外部 DNS サーバ	
		d	CNAME	