平成 28 年度　春期　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
近年，公共機関，金融機関を中心に CSIRT を設立する組織が急増している。インシデントハンドリングは，CSIRT の主要な機能の一つと言える。多くの組織では，CSIRT を設立する以前から，情報システム部門などがインシデントハンドリングに類する活動を行っているが，組織内の役割や権限などが不明確であるため，有効に機能していないケースも散見される。そのような組織では，CSIRT 設立時に，既存のインシデントハンドリングのどのような点を改善するのかを明確にすることが重要である。 本問は，CSIRT の構築とセキュリティ設計を題材に，インシデントハンドリングの問題点を検出して改善する能力，及び脆弱性情報に関する評価能力を問う。

設問		解答例・解答の要点		備考
設問１		a	対応の要否	
設問２	(1)	b	報告すべきインシデントの範囲	
	(2)	インシデントが A 社全体に与える影響度に基づいた対応を指示するため		
設問３	(1)	IT 部の OA 用 PC に攻撃メールが送信され，PC がマルウェアに感染し，起動したマルウェアがサーバ LAN に不正アクセスする攻撃		
	(2)	IT 部運用チームのメンバの LDAP ID 以外によるログイン要求の検知		
設問４	(1)	A 社 IRT が収集すべき脆弱性情報を把握するため		
	(2)	A 社 IRT が，各部署のインシデント発生時や対策時の，影響範囲の特定に活用する。		
設問５		各部署が収集している脆弱性情報の提供を受ける。		
設問６	(1)	現状評価基準		
	(2)	c	ネットワーク	
		d	ローカル	
		e	FW1	

問２

出題趣旨
近年，クラウドサービスやモバイル端末の活用によって業務環境及び業務形態の変化が進んでいる。一方，マルウェアを利用した攻撃はますます巧妙化し，従来型の対策だけでは検知・防御が難しくなっている。そのため，組織においては，クラウドサービスやモバイル端末を意識した検知・防御の仕組みとセキュリティ運用を実現するとともに，侵入されることを前提にした，インシデント対応体制の構築が必要となっている。 本問では，モバイル端末のマルウェア感染を題材に，インシデント発生時の対応能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	UA が DL2 以外の場合には“404 Not Found”を返す。		
	(2)	①	・J プロキシの URL フィルタ機能	
		②	・J プロキシの RH フィルタ機能	
設問２		a	DLL	
設問３	(1)	b	ドライブバイ	
		c	分割	
	(2)	d	・H 社 Web メール	順不同
		e	・N コラボ ・可搬記憶媒体 ・P 社 CRM ツール	
設問４		f	見直し	
設問５	(1)	マルウェアからハードディスク内の情報が透過的に見えてしまうから		
	(2)	①	・AM のマルウェア定義ファイルが初期状態に戻る。	
		②	・セキュリティパッチが適用前の状態に戻る。	
	(3)	画面などの情報からのデータの窃取		
	(4)	項目	3	
		変更後の案	VDI サーバ及び社内 LAN からの HTTP 及び HTTPS 通信によるアクセスだけを許可するよう設定する。	