平成 29 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
最新のウイルス対策システムをもってしても，検知が困難なマルウェアが増えてきており，PC のマルウェア感染はなかなか減少しない。マルウェア感染に迅速に対応するために，情報セキュリティ技術者にとってマルウェアを解析する能力は重要になってきている。 本問では，CSIRT を設置している企業におけるインシデント対応を題材に，マルウェアの動作を解析する能力，及びマルウェア感染による被害を最小限に抑えるための対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	ウ，エ		
	(2)	a	プロキシサーバ	
		b	DHCP サーバ	
設問 2	(1)	被疑サーバの FQDN		
	(2)	中継サーバ 1		
	(3)	被疑サーバへの HTTPS 接続要求を，中継サーバ 1 に到達するようにする。		
設問 3	(1)	実行中プロセスの一覧から既知のデバッガのプロセス名を探す。		
	(2)	暗号鍵を変えてパック処理すると暗号化済みコード部が変化し，ウイルス定義ファイルに登録されていないファイルとなるから		
設問 4	(1)	c	プロキシサーバのブラックリスト	
	(2)	d	脆弱(ぜい)性 K に対応した脆弱性修正プログラムを適用する	
	(3)	e	パスワードの変更	
設問 5	(1)	PDF 閲覧ソフトの脆弱性修正プログラムの適用状況		
	(2)	f	パッチ配信サーバ	
	(3)	PDF 閲覧ソフトの脆弱性修正プログラムを適用する以前に，Q 社の Web サイトを閲覧した場合		
設問 6	(1)	被疑 PC の HDD の複製作業		
	(2)	被疑 PC の解析中に使用する代替 PC の払出し		
	(3)	g	PC 起動時や所定の時刻などに特定のプログラムを自動的に起動する設定内容	

問２

出題趣旨
組織内部のサーバには重要な情報が格納されており，情報漏えい時やマルウェア感染時に組織に与える影響は大きい。しかし，DMZ のサーバと比べると，インターネットから直接攻撃されないという理由から，情報セキュリティ対策が十分に行われないままになっていることがある。 本問では，マルウェア感染を契機とした，社内システムの情報セキュリティ対策強化を題材に，マルウェア感染の影響範囲を調査する能力，及び業務要件を満たす形で情報セキュリティ対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	SMTP over TLS	
	(2)	b	ウ	
		d	ア	
	(3)	c	内部メールサーバ	
設問２	(1)	e	プロキシサーバ	
		f	URL がマルウェア X 中に保持された URL である	
	(2)	g	外部メールサーバ	
		h	インターネット上のサーバに転送された	
	(3)	外部 DNS サーバの設定変更の内容	内部 DNS サーバからの DNS 問合せを拒否する。	
		内部 DNS サーバの設定変更の内容	インターネット上のサーバ名についての DNS 問合せを拒否する。	
	(4)	i	社内専用のドメイン名以外の FQDN が書かれている	
設問３	(1)	ファイルを暗号化しない。		
	(2)	サーバ及び PC でのウイルス検出結果をシステム部運用グループに通知する機能		
設問４		j	PC-LAN	
設問５		業務 LAN の全てのサーバにホスト型 IPS ソフトウェアを導入する。		