平成 25 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 I 試験

問 1

出題趣旨
近年，日本でも被害が報告されている標的型サイバー攻撃に対しては，従来のウイルスや愉快犯によるサイバー攻撃と比べて，攻撃者の攻撃手法やその目的が異なることを念頭において対策することが重要である。 本問では，具体的なマルウェア感染の事例をもとに，マルウェア解析の知識と，標的型サイバー攻撃を受けた際に適切に状況を把握する能力を問う。

設問		解答例・解答の要点		備考
設問 1	(1)	ML2		
	(2)	**機器**	FW	
		ログ	PC から攻撃者のサーバへの HTTP 通信のログ	
設問 2	(1)	a	USB メモリ	
	(2)	攻撃者のサーバの URL を，プロキシサーバのブラックリストに登録する。		
	(3)	PC の Z ブラウザのバージョンを全て 3 にする。		
設問 3	(1)	① ②	・パック処理されていること ・タイムスタンプを変更していること	
	(2)	RD-LAN と他のネットワークとの物理的な隔離		
	(3)	b	新薬の研究報告書を窃取	

問 2

出題趣旨
DNS の名前解決通信は，主に UDP を用いる。UDP は，TCP と比べると送信元 IP アドレスの詐称の検知が難しく，キャッシュポイズニング攻撃の原因ともなっている。ファイアウォールの方式設計においては IP アドレス詐称対策を考慮する必要がある。さらに，インターネットに公開されているサーバの名前解決の方式設計においてはキャッシュポイズニング対策を考慮する必要がある。 本問では，送信元 IP アドレスを詐称した攻撃とその対応を題材にして，ファイアウォール，DNS サーバ及びメールサーバに関する技術要素への理解，設計能力について問う。

設問		解答例・解答の要点		備考
設問 1	(1)	a	UDP	
		b	3way	
		c	DNSSEC	
	(2)	問合せ PT の送信元ポート番号をランダムに変えること		
	(3)	送信元が外部メールサーバの場合，再帰的な名前解決を許可する必要があるから		
	(4)	(d)，(e)，(f)		
	(5)	G 社のドメイン名になりすましたメールを外部メールサーバに送信すること		
設問 2	(1)	IF-1 経由で届く支社プロキシサーバからの正規の問合せ PT と，詐称された問合せ PT とを識別できないから		
	(2)	リゾルバ機能及び DNS キャッシュ機能		

問３

出題趣旨
仮想化技術の進歩によって，デスクトップ仮想化を導入し，リモートアクセス環境を実現する企業が増えている。 本問では，リモートアクセス環境特有のセキュリティリスクとその対策に関する基本的な理解力を問う。また，デスクトップ仮想化の特徴とリスクを理解し，最適なリモートアクセス環境を検討する能力を問う。

設問			解答例・解答の要点	備考
設問１			社外持出し用 PC の紛失や盗難による情報漏えいリスクを低減する効果	
設問２	(1)	a	業務データ	
	(2)	b	ハードディスク暗号化	
	(3)	①	・マスタイメージを再作成する。	
		②	・V-PC の複製を行う。	
		③	・利用者にログオンし直すように周知する。	
設問３			なりすましに成功すると，全ての業務システムを利用できるから	
設問４	(1)	**管理者**	ウイルス定義ファイルの自動配信を設定する。	
		利用者	NT をオフィス LAN に接続する。	
	(2)	**効果**	業務データを端末に保存して社外へ持ち出すことを防ぐ効果	
		理由	V-PC を経由しないと業務システムに接続できないから	

問４

出題趣旨
機密情報保護対策の立案においては，対象となる情報を明確に識別した上で適切な対応を具体化していくことが求められる。 本問では，不正競争防止法の営業秘密の漏えいに関する知識，及び情報漏えいのリスクを識別し漏えい防止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		**要件①**	・秘密として管理されていること	
		要件②	・有用な情報であること	
		要件③	・公然と知られていないこと	
設問２			ディジタルフォレンジックス	
設問３	(1)	a	人事部	
		b	退職日終業時刻	
	(2)	**リスク**	インターネットを利用して機密情報を社外持出し用 PC の外部に送信できる。	
		c	VPN 装置経由だけを許可する	
設問４			ファイルの中身に紙媒体と同様に，“厳秘”，“秘”を明示する。	