平成 20 年度　春期　テクニカルエンジニア（情報セキュリティ）試験　解答例

午後 I 試験

問１

出題趣旨
近年，多数の PC がボットに感染して，迷惑メールや DDoS 攻撃の送信に悪用されている。ボットには，外部から指令を受け取るときに一般業務でも利用する通信ポートを使う機能や，外部から新たなコードをダウンロードして自身のコードを更新する機能など，様々な隠ぺい機能が施されており，ボットに感染した PC を特定する際に，こうした特徴を把握しておくことは重要である。 本問では，迷惑メールの解析，社内ネットワークを踏み台として悪用されないための防御策，ボット感染 PC の追跡に必要な知識と能力を問う。

設問		解答例・解答の要点			備考
設問１	**(1)**	**a**	(ⅰ), (iv)		
	(2)	**d**	ア		
	(3)	(r)			
設問２	**(1)**	**I**	ウ		
		II	イ		
		III	イ		
		α	SMTP		
	(2)	**b**	**方式**	エ	
			仕組み	メール送信時に，パスワードによる認証が行われる。	
		c	**方式**	イ	
			仕組み	POP 認証が成功した後の一定時間内だけメールの送信が可能になる。	
設問３	**(1)**	一般業務で利用する HTTP プロトコルなどの通信ポートを使って指令を受け取ることもできるから			
	(2)	頻繁に自身のコードを更新する。			
	(3)	システムコールを横取りして，その応答を偽装する。			

問２

出題趣旨
システムを運用していく中で，開発時には想定していなかった脅威に直面することがある。情報セキュリティを維持する上では，それらの脅威の影響度に応じて適切な対策を加えていくことが肝要である。 本問では，DoS/DDoS 攻撃の一つである，SYN Flood 攻撃を対象として，その仕組みを確認した上で，攻撃による影響を抑制する方法を問う。

設問		解答例・解答の要点		備考
設問１		**a**	3 ウェイ	
		b	SYN	
		c	SYN/ACK	
		d	ACK	
		e	送信元　又は　ソース	
設問２	**(1)**	大量のハーフオープンによって，ホスト B の資源が占有されるから		
	(2)	TCP の接続開始処理が未完了のものは，Web サーバのアクセスログに記録されないから		
	(3)	同じ送信元 IP アドレスを使って接続要求するとは限らないから		
設問３		ハーフオープン状態の継続時間を制限するためのタイムアウト時間を短くする。		

問3

出題趣旨
現在，各業界の監督官庁又は業界団体から出されている，個人情報保護を目的としたガイドラインにおいては，個人情報を含む通信データの保護を目的として暗号化の実装が求められてきているが，実装方法の検討においては，ガイドラインの内容を理解し，最適な実装方法を検討する必要がある。特に，実装方法の検討においては，製品選択の前に方式による違いを比較検討し，個々の対象箇所に対して最適な方式を選択する必要がある。 本問では，ガイドラインの理解及び通信データ保護のための最適な方式選択において実践的な能力を問う。

設問			解答例・解答の要点	備考
設問1	(1)		光回線を切断して新たに分配器を接続し，ネットワークアナライザを接続する。	
	(2)		通信回線から漏えいする電磁波を解析する。	
設問2	(1)		登録済の MAC アドレスを未登録機器に設定する。	
	(2)	**a**	5	
		b	2	
		c	1	順不同
		d	3	
	(3)	**ア**	端末上では業務アプリケーションが稼働していないから	順不同
		イ	通信プロトコル S は，IP でなく，IP への変更も困難であるから	
		ウ	各取引先の構内ネットワークにおいて，通信回線の終端と外部システム間のネットワークに，ネットワークアナライザを接続されるリスクが残るから	

問4

出題趣旨
マネジメントシステムの構築時に行うリスク対応においては，情報セキュリティに関する知識，論理的思考に基づき，状況を判断し，適切な管理策を選択する能力が求められている。 本問では，ノート PC の社外持出し，外部記憶媒体への不正書出し，サーバへの不正ログインに対する技術的な管理策の知識，論理的思考，判断を問う。

設問			解答例・解答の要点	備考
設問1		**a**	カ	
		b	イ	
		c	ア	
設問2	(1)		ハードディスクを取り外し，その内容をほかの PC で読み出す。	
	(2)		・ハードディスク上の情報を暗号化する。 ・ハードディスクにアクセスパスワードを設定する。	
設問3			・セキュリティツールを導入して，外部記憶媒体への書出しを禁止する。 ・外部記憶媒体への書出しができないドライバソフトに入れ替える。 ・OS の設定によって，外部記憶媒体への書出しを禁止する。	
設問4	(1)	**d**	イ	
		e	オ	
	(2)	①	・パスワードの有効期間	
		②	・パスワードの複雑さ	
		③	・パスワードの履歴の保存数 ・パスワードの変更禁止期間	
	(3)		・同じパスワードでもソルトが異なるとハッシュ値が変わるから ・攻撃者がソルトの値ごとにテーブルを用意する必要があるから	