平成 27 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
標的型攻撃の事例として，就職活動者を装い，採用担当として公開されている問合せ用メールアドレス宛てにウイルスを含むファイルを送り付ける手口が報告されている。そういった手口に対抗するためには，ウイルス対策について有効性を常に確認し継続的に見直していくことが重要である。 本問では，休暇明けのウイルス感染を題材に，システム管理者が実施するウイルス対策能力，及びメールによる問合せ受付の代替としての Web フォームによる問合せ受付機能の設計能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	DNSSEC	
	(2)	b	オープン	
		c	エンベロープ	
	(3)	d	n-sha.co.jp	
設問２		e	送信者メールアドレス	
設問３		脆弱性修正プログラム及びウイルス定義ファイルを提供するサイトに制限する。		
設問４	(1)	初期設定用ネットワークに接続し，W 社の駆除ツールをダウンロードして適用した。		
	(2)	中継サーバのサーバ名を部分一致でマッチさせる。		
	(3)	G さん以外の広報グループのメンバに届いたメールを調査し，マルウェア X を含むメールを削除した。		
	(4)	スキャン不能の場合も通知するようにした。		
設問５		① ②	・1 週間を超えてフルスキャンが実行されない PC を指定して，フルスキャンを実行させる。 ・ウイルス定義ファイルが更新されない PC を指定して，ウイルス定義ファイルを更新させる。 ・アップロードされるウイルス感染情報を基に感染した PC を特定し，ウイルスを駆除する。	
設問６	(1)	連絡用メールアドレス	攻撃対象のメールアドレス	
		お問合せ内容	誘導する Web サイトの URL	
	(2)	f	・hhttp://ttp ・hhttp://ttps ・hhttps://ttp ・hhttps://ttps	

問２

出題趣旨
製造装置，医療機器などには，汎用 OS を利用しているにもかかわらず，脆弱性修正プログラムを適用できない機器が存在している。これらの機器は，脆弱性の存在を前提として稼働を続けなければならない。このような状況で，個々の業務の状況に応じて安全な稼働を実現するための対策を決定することが求められている。 さらに，近年の製造業者及び医療機関においては，他の組織とのネットワーク接続を迫られている。このようなネットワークを活用して，安全で使いやすいシステムを構築することがセキュリティ技術者に対して与えられた課題である。 本問では製造業における製造装置の LAN 接続を題材として，これらの課題について対策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		a	事務系 LAN への接続時にマルウェアに感染した転送用 PC を，その状態のままで製造系 LAN へ接続すると，製造装置へマルウェアの感染が広がる。	
設問２	(1)	b	操作禁止状態に	
		c	他人が推測できない	
		d	知られないように	
	(2)	e	影響を評価し，必要であれば脆弱性修正プログラムを適用する	
設問３		f	情報共有系 LAN と製造系 LAN の間で通信が成立することがない。	
		g	情報共有系 LAN 上の機器へ実行形式ファイルが書き込まれても，製造系 LAN にファイルが転送されることがない。	
設問４	(1)	① ②	・IP アドレスが動的に割り当てられるインターネット回線を利用している協力会社に対応できない。 ・プロキシサーバを利用している協力会社の場合，社内の接続端末の個別識別ができない。	
	(2)	h	K 工場	
		i	K 工場	
		j	J 社本社	
		k	K 工場	
		l	J 社本社	
	(3)	K サーバへのアクセスだけに使用する鍵ペアだから		
	(4)	① ②	・証明書に対応した秘密鍵の漏えいが疑われる場合 ・接続端末を廃棄する場合	