平成 31 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
情報システムのセキュリティを確保するためには，脆弱性，攻撃手法及び対策手法を正しく理解しておくだけでなく，新たな脆弱性が発見されたときに，その脆弱性に応じて適切な対策を選択できるようにしておく必要がある。 本問では，無線 LAN の脆弱性を題材に，攻撃手法と脆弱性を理解する能力，及び対策を立案し，効果を評価する能力を問う。

設問		解答例・解答の要点		備考
設問 1		a	FW1	
		b	プロキシサーバ	
設問 2		内容	削除されたファイルの内容	
		手段	空きセクタの情報からファイルを復元する。	
設問 3	(1)	MAC アドレスが平文の状態で送信されるから		
	(2)	端末の無線 LAN ポートの MAC アドレスを，総務部の W-AP に登録済みの MAC アドレスに変更する。		
設問 4	(1)	IP ヘッダ部及び TCP ヘッダ部は，同一のバイト列であることが多いこと		
	(2)	c	同一の暗号ブロック	
		d	平文ブロック	
		e	カウンタ値を暗号化した値	
設問 5	(1)	f	読み取る	
	(2)	g	カ	
		h	オ	
	(3)	① ②	・攻撃者が用意した W-AP に接続し，情報を送信する。 ・内部メールサーバを利用して攻撃者にメールを送信する。	
設問 6	(1)	i	信頼する CA のディジタル証明書	
	(2)	j	クライアント証明書の提示が必要な外部 Web サーバにアクセスする。	
	(3)	k	FW1 の製造元によって安全性が確認されていない CA が発行したサーバ証明書を使用した外部 Web サーバにアクセスする。	

問２

出題趣旨
サイバー攻撃は，年々，巧妙化している。攻撃者は，情報セキュリティ対策が不十分な取引先にまず侵入し，そこから大企業の重要な情報を狙うようになった。そこで，自社だけでなく取引先を含めた情報セキュリティ対策が必要になっている。 本問では，取引先にも影響を及ぼしたセキュリティインシデントへの対応を題材に，PC 及びサーバのセキュリティ対策の設計能力を問う。

設問		解答例・解答の要点		備考
設問１		a	秘密管理	
		b	有用	
		c	非公知	
設問２	(1)	d	オープンリレー	
	(2)	x1.y1.z1.16/29		
設問３	(1)	e	x1.y1.z1.18	
	(2)	f	NTP	
	(3)	g	ア	
	(4)	h	CRYPTREC	
設問４		i	エ	
設問５	(1)	なりすましによるアクセスの場合，操作した人物とログに記録された利用者 ID の利用者とは異なるから		
	(2)	アクセスがあった時，共同出品担当メンバは B 社にいて K さんの DPC を使用できないこと		
	(3)	パスワードを変更する。		
	(4)	マルウェア X を含む圧縮ファイルを保存している DPC の有無を確認するため		
	(5)	圧縮ファイルを展開すると，展開したファイルに対してリアルタイムスキャンが実行されるから		
設問６	(1)	アクセスを許可する IP アドレスとして，設計部 LAN 及び製造部 LAN だけを登録する。		
	(2)	初期パスワードは，利用者ごとに異なるランダムな文字列にする。		
設問７		j	管理者に通知	