令和元年度　秋期　情報処理安全確保支援士試験　解答例

午後Ⅰ試験

問1

出題趣旨
昨今，なりすましメールによって企業機密や金銭をだまし取られるなどの被害が発生しており，その対策として，送信ドメイン認証技術を普及させようという働きかけがある。 本問では，送信ドメイン認証技術の基礎知識を含め，実際の業務において与えられた環境に送信ドメイン認証技術を適切に適用する能力を問う。

設問		解答例・解答の要点		備考
設問1		a	MAIL FROM	
設問2	(1)	b	×	
		c	×	
		d	×	
		e	×	
		f	×	
		g	○	
		h	×	
		i	×	
	(2)	j	x1.y1.z1.1	
	(3)	送信側の DNS サーバに設定された IP アドレスと SMTP 接続元の IP アドレスが一致しないから		
	(4)	メール本文及びメールヘッダの改ざんの有無		
設問3		k	mail.x-sha.co.jp.	
		l	x2.y2.z2.1	
		m	quarantine	
		n	r	
設問4		N 社の取引先と似たメールアドレスから送信ドメイン認証技術を利用してメールを送信する。		

問２

出題趣旨
最近，攻撃対象組織ごとにマルウェアなどを用意する攻撃が増えている。そういった攻撃に対応するため，ISAC などの脅威インテリジェンスを共有する組織を活用し，インシデント対応を行うケースが増えている。 本問では，脅威インテリジェンスの関連知識と脅威インテリジェンスを活用するインシデント対応力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	プロキシ認証に失敗したから		
	(2)	a	(b)	
	(3)	① ②	・グローバル IP アドレス M への HTTP 通信成功のログ ・パブリック DNS サービス L への DNS 通信成功のログ	
	(4)	① ②	・イ ・ウ	
設問２	(1)	エ		
	(2)	ウ		
	(3)	項番	3	
		送信元	DMZ	
		宛先	インターネット	
		サービス	DNS	
		動作	許可	
	(4)	b	権威 DNS サーバ	
		c	外部 DNS サーバ	
		d	再帰的クエリ	
	(5)	e	特定のドメインに対する多数の DNS クエリの発生	

問３

出題趣旨
最近の標的型メール攻撃は巧妙になっており，セキュリティ製品を導入することや，不審な添付ファイルや不審なリンク先をクリックさせないなど，利用者へ注意喚起することでは，被害の完全な抑止は難しい。 本問では，一般的なネットワーク構成におけるウイルス感染を題材として，ウイルスの関連知識とウイルス感染後のインシデント対応力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	メモリ上の情報が失われないようにするため		
	(2)	① ②	・J 社情報システムに感染を拡大する。 ・インターネットに情報を送信する。	
設問２		a	ウ	
		b	イ	
		c	オ	
		d	ア	
設問３	(1)	e	IP アドレス w1.x1.y1.z1 との通信履歴	
	(2)	感染したが，C&C サーバと通信する前にネットワークから切り離された状態		
	(3)	R ログをマルウェア M のハッシュ値で検索する。		