平成 30 年度　秋期　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
クラウドサービスが普及している一方，企業・組織にはクラウド環境に移行できないシステムも存在している。このような背景から，当面，企業・組織は，オンプレミス環境とクラウド環境が併存するハイブリッドクラウド環境においてシステムを運用する必要性に迫られている。ハイブリッドクラウド環境においても，セキュリティの確保は重要な考慮点であるが，ハイブリッドクラウド環境のセキュリティ設計においては，クラウド環境に移行すべきシステムの選定，ハイブリッドクラウド環境における利用者 ID 管理及びアクセス管理，クラウド環境におけるエンドポイント管理，モバイル環境の考慮といった点がしばしば議論になる。 本問では，ハイブリッドクラウド環境におけるセキュリティ設計に関する知識と能力を問う。

設問		解答例・解答の要点		備考
設問 1		GDPR		
設問 2	(1)	R&D 情報は，物理的な入退室管理が行われているプロジェクトルーム内に配置されたプロジェクト専用サーバに保管する。		
	(2)	満たせなくなる基本要件の具体的内容	①・生産関連サーバは，X 社の工場及びデータセンタに配置する。 ②・生産関連サーバのバックアップを他の工場又はデータセンタに配置する。 ③・同じ重要インフラ設備を製造する工場及び生産関連サーバは同一の国又は地域内の 2 か所以上に配置する。	
		IaaS C のサービス仕様の内容	日本国内のデータセンタが被災した場合はシンガポールのデータセンタでサービスが継続される。	
	(3)	X 社のシステムの機器に割り当てている IP アドレスが，IaaS C で予約されているプライベートアドレスと重複する可能性があるという問題		
設問 3	(1)	一度のログインで全システムにアクセスできるという利便性		
	(2)	業務サーバ	㋑，㋒	
		構成要素	㋕，㋖，㋘，㋙	
設問 4	(1)	ティア 1	イ	
		ティア 2	ウ	
		ティア 3	ア	
	(2)	標準ソフトウェア以外のソフトウェアは，脆弱(ぜい)性管理がされないという不都合		
	(3)	①・正確である。 ②・作業が速くできる。		

設問 5 (1)

		クライアント	業務サーバ	備考
案 A	①	Ⓗ	Ⓓ	
	②	Ⓘ	Ⓓ	
案 B	①	Ⓖ	Ⓑ	
	②	Ⓗ	Ⓑ	
	③	Ⓘ	Ⓑ	

設問 5 (2)		備考
a	カ	
b	ウ	
c	イ	
d	ア	
e	オ	
f	ク	
g	キ	
h	エ	

問２

出題趣旨
サイバー攻撃の技術は高度化し，攻撃者の侵入を完全に防ぐことはますます困難になってきた。これに伴い，セキュリティインシデント（以下，インシデントという）となり得る事象を素早く検知し，調査し，対処する能力の重要性が高まっている。 本問では，マルウェアの侵入に端を発した情報漏えいインシデントを題材として，インシデント対応をスムーズに行うための仕組みを検討して構築する能力と，ログやそのほかの情報を組み合わせて，インシデントの全容を整理し，理解する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	エ	順不同
		b	イ	
	(2)	c	ケ	
		d	ウ	
		e	コ	
設問２	(1)	f	ログを取得する機器	順不同
		g	取得するログの種類	
		h	保存期間	
	(2)	i	タイムゾーン	
		j	統一	
	(3)	ネットワークトラフィック量と比較して異常を検知する。		
設問３	(1)	プロキシサーバのログからアクセス先がサイト M のエントリを抽出し，このエントリから PC-A の IP アドレスを得た。		
	(2)	HTTP リクエストによる活動	C&C サーバへのコマンド要求又は応答	
		HTTP レスポンスによる活動	C&C サーバからのコマンド受信	
	(3)	問題	PC のネットワークインタフェースや通信の状態についての情報が失われること	
		措置	メモリダンプを取得する。	
	(4)	k	プロキシサーバのログから，IPn のサイトにアクセスした機器がほかにないか	
	(5)	7 回		
	(6)	l	ハッシュ値	
	(7)	行番号	28 行目	
		役立つ情報	プロキシサーバがインターネットに送信したデータのサイズ	
設問４	(1)	ア	9／4　14：31	
		イ	9／4　14：37	
		ウ	9／5　10：41	
	(2)	m	タ	
		n	コ	
		o	ソ	
		p	ケ	
		q	シ	
		r	カ	
		s	オ	
設問５		課題	b	
		措置	インシデント対応の作業手順書を作成する。	