令和３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
サイバー攻撃の被害拡大防止のためには，ID 管理，ネットワークフィルタリング，ログ管理などの複数の対策で対処する必要がある。 本問では，リモート保守のセキュリティインシデント対応をきっかけとした，被害範囲の調査並びに SSH サーバ及びファイアウォール設定の見直しを題材に，ログ及び認証・認可といった複数の対策を組み合わせての設計能力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	接続先が保守用中継サーバではない	
	(2)	操作ログの改ざんや削除を防止するため		
	(3)	b	保守 PC-A	
		c	インターネット	
設問２	(1)	6		
	(2)	6 月 14 日の 7 時 0 分から 6 月 14 日の 9 時 30 分まで		
設問３	(1)	・保守員以外が不正に秘密鍵を利用できないようにするため ・秘密鍵が盗まれても悪用できないようにするため		
	(2)	d	パスワード認証	
	(3)	e	秘密鍵	
	(4)	f	送信元 IP アドレスを固定にする	

問２

出題趣旨
昨今，利用者のミスによる情報漏えいのほか，内部からの意図的な持出しや外部からの攻撃者の侵入など，様々な要因で秘密情報が外部に漏えいするリスクが高まっている。 本問では，設計文書の管理における問題の調査及び IRM（Information Rights Management）の導入を題材に，情報漏えいリスクを特定し，適切に対策する能力について問う。

設問		解答例・解答の要点		備考
設問１		a	P パスワードの変更	
		b	PC にコピー	
設問２	(1)	アカウント	ア，イ	
		操作	プロジェクト離任者の利用者アカウントをグループから削除する。	
	(2)	(ii)		
	(3)	c	60	
		d	196	
	(4)	e	辞書	
	(5)	f	多要素認証	
設問３		利用者がファイルを開いたとき，画面をキャプチャし，攻撃者に送信する動作		

問３

出題趣旨
組織内のサーバは，インターネットから直接攻撃できないという理由から，DMZ のサーバと比較し，情報セキュリティ対策が不十分なままになっていることがあるが，そのことによってセキュリティインシデントの被害が拡大することも少なくない。 本問では，組織内の PC のマルウェア感染をきっかけとした，情報漏えいの有無の調査並びにファイアウォール及びサーバ設定の見直しを題材に，調査能力及びサーバの設計能力を問う。

設問		解答例・解答の要点			備考
設問１	(1)	LAN から切り離す。			
	(2)	ディスクイメージ			
	(3)	a	最新のマルウェア定義ファイルを保存した DVD-R の使用		
		b	マルウェア定義ファイルの更新		
		c	マルウェア対策ソフトの画面の操作		
	(4)	Q 社内の全ての PC 及びサーバからのアクセス			
設問２	(1)	①	項番	3	
			送信元	総務部 LAN，営業部 LAN	
		②	項番	4	
			送信元	技術部 LAN	
	(2)	d	V 社配布サイトの URL		
		e	全て		
設問３	(1)	登録した実行ファイルがバージョンアップされた場合			
	(2)	登録した実行ファイルのマクロとして実行されるマルウェア			